AUTOMORPHISMS OF FINITELY GENERATED NILPOTENT GROUPS

by

Ursula Hilda Mary Webb

submitted for the degree of Ph.D. in October 1978

Mathematics Institute

University of Warwick

Coventry

Acknowledgements

I should like to thank my supervisor Dr S.E. Stonehewer for his advice and encouragement during the past two years. I am grateful to Dr J. Hulse for drawing attention to the problem and to the Science Research Council for financial support.

Declaration

Chapters 1 and 2 contain an account of work due to various authors except for theorem 2.2.6 which seems to be my own. I believe the material presented in chapters 3 , 4 and 5 to be original.

SUMMARY

If G is a finitely generated nilpotent group then it appears to be an open question whether G admits a non-inner automorphism. In chapter 1 we survey what is known about the problem and explain why it suffices to consider the case where G has Hirsch length one. In chapter 2 we survey how group cohomology has been used in the study of group automorphisms and use this theory to show that if a group G has an infinite cyclic subgroup C of finite index and G/C admits a non-inner automorphism which centralises its derived quotient then this automorphism lifts to a non-inner automorphism of G.

In chapter 3 we show that finding a finitely generated nilpotent group which admits no non-inner automorphism acting nilpotently is equivalent to finding a pair (T,ϕ) where T is a finite p-group and ϕ is an automorphism of T of p-power order such that $|C_{\mathrm{Out}T}(\bar{\phi}):\langle\bar{\phi}\rangle|$ is coprime to p and $[\phi,\langle c,Z(T)\rangle] = Z(T)$ where $\langle\phi\rangle \cap \mathrm{Inn}T = \langle\mu_c\rangle$. We analyse such pairs in chapter 4 by looking at the $K\langle\phi\rangle$ module structure of certain subgroups of $\mathrm{Aut}T$ where K is the field of p elements. Chapter 5 contains our main results; that a finitely generated nilpotent group of Hirsch length one admits a non-inner automorphism acting nilpotently if its torsion subgroup has nilpotency class two, or has exponent p, or is of maximal class or (if $p \neq 2$) has cyclic derived group.

CONTENTS

Chapter One Introduction

The student of group automorphisms would like to obtain a description of the automorphism group, AutG , of a group G . InnG , the group of automorphisms of G induced by conjugation by elements of G , is isomorphic to G factored by its centre, and so our student first studies OutG , the quotient of AutG by InnG . It is in general hard to calculate OutG or even to determine its elementary properties, and recent research has concentrated on discovering when OutG can be trivial , that is, what groups admit no non-inner automorphisms. Such groups are called semicomplete.

If G is a group with trivial centre then G is isomorphic to InnG , and G embeds in AutG , which also has trivial centre. If further G is semicomplete G is said to be complete; the smallest non-trivial complete group is the symmetric group on three letters. Wielandt has shown [12] that any finite group G with trivial centre embeds subnormally in a complete group, in the following way. We define a tower of groups $\{W_i \; i \geqslant 1\}$ by $W_1 = G$, $W_i = \mathrm{Aut}W_{i-1}$ for $i \geqslant 2$. Then each W_i has trivial centre and embeds as a normal subgroup of W_{i+1} . Then Wielandt shows that the tower terminates, that is that the W_i are equal from some point on. Notice that a complete group is isomorphic to its automorphism group but the converse is not true ; for example the dihedral group of order eight is isomorphic to its automorphism group but does not have trivial centre.

The situation for semicomplete groups with non-trivial centre is rather more opaque, and in 1955 Schenkman and Haimo [8] conjectured that a nilpotent group of order at least three could never be semicomplete. This conjecture has been verified for periodic nilpotent groups, in the finite case by Gaschütz [2,3] and in the infinite case by Zalesskii [13] .(There appear to be some errors in Zalesskii's paper but these have been corrected by Stonehewer). We shall give an alternative proof of Gaschütz result in chapter 2, following Schmid [9] .

However the conjecture is false for non-periodic groups as is shown by examples due to Zalesskii [14] and Heineken [6] . They show that many semicomplete groups exist and produce a semicomplete group H which is torsion free and extraspecial, that is,its centre $Z(H)$ is infinite cyclic and equal to its derived group. H is not finitely generated, and indeed no example is known of an infinite nilpotent semicomplete group which is finitely generated. This leads us to restrict our attention to finitely generated nilpotent groups, and to ask whether such a group (apart from C_2) can ever be semicomplete.

We record some information about a finitely generated nilpotent group G . G is polycyclic and so the number of infinite cyclic factors in any cyclic series for G is the same; this number is the Hirsch length of the group, denoted by $h(G)$. Any subgroup N of G is finitely generated and if N is normal in G then $h(G) = h(G/N) + h(N)$. The elements of finite order in G form a finite characteristic subgroup of G , the torsion subgroup T . G/T is torsion free nilpotent and finitely generated and $h(G/T) = h(G)$.

If α is an automorphism of a nilpotent group G we say that α acts nilpotently on G if $G \rtimes \langle\alpha\rangle$, the split extension of G by $\langle\alpha\rangle$, is nilpotent. Let $\mathrm{Nil}G$ be the set of all such automorphisms; obviously $\mathrm{Nil}G$ contains $\mathrm{Inn}G$. One may verify that an automorphism α of a nilpotent group G acts nilpotently on G if and only if there exists a series $1 = G_0 \lhd \ \dots \ \lhd G_n = G$ of α-invariant subgroups G_i of G such that α centralises G_i/G_{i-1} for all $1 \leq i \leq n$. It follows that if A is a normal subgroup of G normalised by an automorphism α of G then α lies in $\mathrm{Nil}G$ if and only if $\alpha|_A$ lies in $\mathrm{Nil}A$ and $\alpha|_{G/A}$ lies in $\mathrm{Nil}G/A$.

If G is a finite p-group then $\mathrm{Nil}G$ is just the set of all automorphisms of G of p-power order. Gaschutz showed that any finite p-group which is not of prime order admits a non-inner automorphism acting nilpotently, and it follows from this that any finite nilpotent group which is not a product of groups of distinct prime orders admits a non-inner automorphism acting nilpotently.

If G is a finitely generated nilpotent group with Hirsch length at least two then as Baumslag shows in [1], G has an outer automorphism acting nilpotently. The following proof is due to Stonehewer.

G/T is a torsion free nilpotent group so we can pick N, a normal subgroup of G such that N contains T and G/N is infinite cyclic. Then $h(N) = h(G) - h(G/N)$ so $h(N)$ is at least one and N is an infinite finitely generated nilpotent group, in particular $Z(N)$ is infinite. G is nilpotent so $[G,Z(N)]$ is a proper subgroup of $Z(N)$ and since $Z(N)$ is an infinite abelian group we can pick an element y of $Z(N)$ with the property that y has infinite order and does not lie in $[G,Z(N)]$. Let x be an element of G such that $G = \langle x,N \rangle$. Define a map $\theta : G \longrightarrow G$ by $x\theta = xy$, $n\theta = n$ for all n in N ; θ is an automorphism of G . If θ is conjugation by $x^i u$ for some $i \in \mathbb{Z}$, $u \in N$, then we have $[N,x^i u] = 1$ and

$$[x,x^i u] = y .$$

It follows that

$$[Z(N),x^i] = 1 \qquad (1)$$

$$[u\ ,x^i] = 1 \quad \text{and} \qquad (2)$$

$$[x,u] = y .$$

Let $W = \langle u,Z(N) \rangle$. As u lies in N , W is abelian. W is normalised by x , since $Z(N)$ is normal in G and $u^x = uy^{-1}$ which lies in W as y lies in $Z(N)$. (1) and (2) show that x centralises W .

We want to apply the following lemma.

<u>Lemma</u> Let H be a nilpotent group and let z be an element of H which normalises an abelian subgroup V of H . Suppose that some power of z centralises V . Then $[z,v]$ has finite order for all $v \in V$.

<u>Proof</u> Let j be an integer such that z^j centralises V . The proof is by induction on the nilpotency class of H . If H is abelian the result is obvious. So suppose that H is not abelian, and let bars denote images modulo $Z(H)$. The hypotheses of the theorem hold for $\bar{V}$ and $\bar{z}$ in $\bar{H}$ so given an element v of V there exists an integer t such that $[z,v]^t$ lies in $Z(H)$.

Now V is abelian so $[z,v]^v = [z,v]$ and thus

$$[z,v]^t = [z,v^t] .$$

Then $\quad 1 = [z^j,v^t]$ by hypothesis

$= [z,v^t]^j$ as $[z,v^t]$ lies in $Z(H)$

$= [z,v]^{tj}$ and so $[z,v]$ has finite order.

Applying this lemma with $G = H$, $V = W$ and $x = z$ we deduce that $[x,u] = y$ has finite order. But this contradicts our choice of y , so the automorphism θ must be a non-inner automorphism of G .

Notice that θ centralises the series $1 \lhd N \lhd G$ of G so θ acts nilpotently and we have shown that any finitely generated nilpotent group with Hirsch length at least two admits a non-inner automorphism which acts nilpotently.

So in investigating the conjecture of Schenkman and Haimo for finitely generated nilpotent groups we need to consider groups of Hirsch length one. If such a group is torsion free it is isomorphic to the infinite cyclic group and its automorphism group is of order two, generated by the automorphism which maps every element of the infinite cycle to its inverse. This automorphism does not act nilpotently. However it is not known whether there exists a non-cyclic finitely generated nilpotent group of Hirsch length one which is semicomplete, or even if there exists one which admits no non-inner automorphisms acting nilpotently. This is the question we study in this essay.

Stonehewer and Gupta [10] have shown that an infinite two generator nilpotent group of class at most four admits a non-inner automorphism acting nilpotently. They use combinatorial techniques which can probably be generalised to cope with other cases.

The main purpose of this essay is to show that an infinite, non-cyclic, finitely generated nilpotent group whose torsion subgroup has nilpotency class two admits a non-inner automorphism which acts nilpotently. Rather than proceeding directly to the result however we describe more general techniques and give examples of their use in tackling other classes of finitely generated nilpotent groups. For example we show that an infinite non-cyclic finitely generated nilpotent group whose torsion subgroup is of exponent p, or of maximal class, or has cyclic derived group and order not a power of 2, admits a non-inner automorphism acting nilpotently. Our results are stated in full in 5.4.

The usual techniques used in the study of group automorphisms are cohomological, and we survey these in chapter 2 explaining how they might be useful for our purposes. Rather than developing them further however we adopt a non-cohomological approach and this is given in chapters 3 to 5, leading to a consideration of the case when the torsion subgroup has class 2 in section 5.2.

Chapter 2 Automorphisms and group cohomology

The study of group automorphisms is hampered by a lack of theorems which give conditions for an automorphism of a subgroup to lift to an automorphism of the whole group. Since whether a particular automorphism lifts depends not only on the subgroup and the quotient group. but also on the particular extension involved, questions in extension theory and thus in group cohomology arise.

In section 1 we give an account of this theory, incorporating the work of several authors. In section 2 we apply the theory to central automorphisms to deduce theorems due to Robinson. We use these theorems to obtain results about a class of groups which includes finitely generated nilpotent groups of Hirsch length one; in particular we show that certain automorphisms of finite quotients of these groups lift to automorphisms of the whole group. Section 3 contains an account of Schmid's proof of Gaschütz' theorem, which depends on a lifting theorem derived from the work in section 1.

Section 2.1

Suppose we are given a group G and a normal subgroup N of G. Let $Q = G/N$. We want to know what we can say about $\mathrm{Aut}G$ in terms of $\mathrm{Aut}N$ and $\mathrm{Aut}Q$. We shall denote by $N_{\mathrm{Aut}G}(N)$ the group of automorphisms of G which normalise N. As N is normal in G $\mathrm{Inn}G$ lies inside $N_{\mathrm{Aut}G}(N)$, and $\mathrm{Aut}G = N_{\mathrm{Aut}G}(N)$ whenever N is characteristic in G. Any element of $N_{\mathrm{Aut}G}(N)$ induces automorphisms of N and Q and so we get a map $\Gamma: N_{\mathrm{Aut}G}(N) \longrightarrow \mathrm{Aut}Q \times \mathrm{Aut}N$ defined by $\Gamma: \alpha \longrightarrow (\alpha|_Q, \alpha|_N)$ for all α in $N_{\mathrm{Aut}G}(N)$. The kernel of Γ is the group of those automorphisms of G which normalise N and induce the identity on Q and N; we denote this group by $C_{\mathrm{Aut}G}(G/N,N)$. Thus we get an exact sequence

$$1 \longrightarrow C_{\mathrm{Aut}G}(G/N,N) \longrightarrow N_{\mathrm{Aut}G}(N) \xrightarrow{\Gamma} \mathrm{Im}\Gamma \longrightarrow 1 .$$

Our aim in this section is to provide alternative descriptions of $C_{\mathrm{Aut}G}(G/N,N)$ and $\mathrm{Im}\Gamma$. First we look at $C_{\mathrm{Aut}G}(G/N,N)$. As N is normal in G, $\mathrm{Inn}G \leq N_{\mathrm{Aut}G}(N)$. If H is a subgroup of G we let $H\mu$ denote the group of automorphisms of G induced by conjugation by elements of H; if $h \in H$ we let μ_h denote conjugation by h. If $G/N = Q$ and A is the subgroup of G containing N with $A/N = Z(Q)$ then $\mathrm{Inn}G \cap C_{\mathrm{Aut}G}(G/N,N) = (A \cap C_G(N))\mu$. The following lemma is well known (see e.g. [5]).

2.1.1 <u>Lemma</u> Suppose that N is a normal subgroup of a group G. Then $C_{\mathrm{Aut}G}(G/N,N)$ is isomorphic to $Z^1(G/N,Z(N))$ and under this isomorphism $Z(N)\mu$ corresponds to $B^1(G/N,Z(N))$.

2.1.2 <u>Corollary</u> Suppose that $C_G(N) = Z(N)$. Then $H^1(G/N,Z(N)) \cong C_{AutG}(G/N,N)/InnG \cap C_{AutG}(G/N,N)$, and if $H^1(G/N,Z(N)) \neq 1$ then $C_{AutG}(G/N,N)$ does not lie in $InnG$.

<u>Proof</u> $H^1(G/N,Z(N))$ is just $Z^1(G/N,Z(N))/B^1(G/N,Z(N))$, so the previous lemma shows that $H^1(G/N,Z(N)) \cong C_{AutG}(G/N,N)/(Z(N)\mu)$. But if $A/N = Z(Q)$ then $A \cap C_G(N) = A \cap Z(N) = Z(N)$ so $(Z(N)\mu) = InnG \cap C_{AutG}(G/N,N)$ by the remarks above.

To enable us to describe $Im\Gamma$ we examine the set of extensions of N by Q . Let

$E : 1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} Q \longrightarrow 1$

be an extension of N by Q , and let π be the projection of G onto Q . E defines a map $\rho : G \longrightarrow AutN$ where for any g in G , $g\rho$ is the automorphism of N induced by conjugation by g . We associate to E the map $\chi : Q \longrightarrow OutN$ where χ is defined so as to make the following diagram commute.

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, "\pi"'] & AutN \arrow[d] \\ Q \arrow[r, "\chi"] & OutN \end{tikzcd}$$

χ is called the coupling of E . Suppose that

$E_1 : 1 \longrightarrow N \longrightarrow G_1 \longrightarrow Q \longrightarrow 1$

is another extension of N by Q . We say that E and E_1 are equivalent if there exists an isomorphism $d : G \longrightarrow G_1$ such that the following diagram commutes.

$$\begin{tikzcd} & & G \arrow[dd, "d"] \arrow[dr] & & \\ 1 \arrow[r] & N \arrow[ur] \arrow[dr] & & Q \arrow[r] & 1 \\ & & G_1 \arrow[ur] & & \end{tikzcd}$$

We denote the equivalence class of the extension E by $[E]$. Equivalent extensions determine the same coupling.

Let $\mathcal{E}(N,Q)$ be the set of equivalence classes of extensions of N by Q , and $\frac{Q}{N,\chi}$ the subset of $\mathcal{E}(N,Q)$ consisting of equivalence classes with coupling χ . The following well-known result can be found in [5] .

2.1.3 <u>Theorem</u> If $\frac{Q}{N,\chi}$ is non-empty then its elements are in one-one correspondence with those of $H^2(Q,Z(N))$.

We now determine an action of $\mathrm{Aut}Q \times \mathrm{Aut}N$ on $\mathcal{E}(N,Q)$.

Let

$$E : 1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1$$

be an extension of N by Q , and let (σ,ν) be an element of $\mathrm{Aut}Q \times \mathrm{Aut}N$. Define $E(\sigma,\nu)$ to be the extension

$$E(\sigma,\nu) : 1 \longrightarrow N \xrightarrow{\nu^{-1}.i} G \xrightarrow{\pi\sigma} Q \longrightarrow 1 \quad .$$

If E has coupling χ then $E(\sigma,\nu)$ has coupling $\chi_{\sigma,\nu}$ determined by the following diagram

$$\begin{tikzcd}
G \arrow[r, "\rho"] \arrow[d, "\pi"'] & \mathrm{Aut}N \arrow[r, "\mu_\nu"] \arrow[d] & \mathrm{Aut}N \arrow[d] \\
Q \arrow[r, "\chi"] \arrow[d, "\sigma"'] & \mathrm{Out}N \arrow[r, "\bar{\mu}_\nu"] & \mathrm{Out}N \\
Q \arrow[urr, "\chi_{\sigma,\nu}"'] & &
\end{tikzcd}$$

where μ_ν denotes conjugation by ν in $\mathrm{Aut}N$ and $\bar{\mu}_\nu$ is the automorphism of $\mathrm{Out}N$ induced by μ_ν . Thus $\chi_{\sigma,\nu} = \sigma^{-1}\chi\,\bar{\mu}_\nu$, and we can use this to define an action of (σ,ν) on any element of $\mathrm{Hom}(Q,\mathrm{Out}N)$.

We can check that this action induces an action of $\mathrm{Aut}Q \times \mathrm{Aut}N$ on $\mathcal{E}(N,Q)$, and that under this action (σ,ν) in

$\mathrm{AutQ} \times \mathrm{AutN}$ maps $\frac{Q}{N,\chi}$ onto $\frac{Q}{N,\chi_{\sigma,\tau}}$ for each $\chi \in \mathrm{Hom}(Q,\mathrm{OutN})$. Given $\chi \in \mathrm{Hom}(Q,\mathrm{OutN})$ the subgroup S_χ of $\mathrm{AutQ} \times \mathrm{AutN}$ acts on $\frac{Q}{N,\chi}$ where $S_\chi = \mathrm{Stab}_{\mathrm{AutQ} \times \mathrm{AutN}}(\chi)$.

The following lemma enables us to identify $\mathrm{Im}\,\Gamma$.

2.1.4 Lemma Let

$$E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

be an extension of N by Q with coupling χ , and let $\Gamma : N_{\mathrm{AutG}}(N) \longrightarrow \mathrm{AutQ} \times \mathrm{AutN}$ be defined as above. Let $\mathrm{AutQ} \times \mathrm{AutN}$ act on $\mathcal{E}(N,Q)$ and S_χ act on $\frac{Q}{N,\chi}$ as defined above. Then

$$\mathrm{Im}\,\Gamma = \mathrm{Stab}_{\mathrm{AutQ} \times \mathrm{AutN}}([E]) = \mathrm{Stab}_{S_\chi}([E]) .$$

Proof We show first that if $(\sigma,\tau) \in \mathrm{AutQ} \times \mathrm{AutN}$ stabilises $[E]$ then (σ,τ) lies in S_χ ; this shows that $\mathrm{Stab}_{\mathrm{AutQ} \times \mathrm{AutN}}([E]) = \mathrm{Stab}_{S_\chi}([E])$. So suppose that (σ,τ) stabilises $[E]$, that is that $E(\sigma,\tau)$ is equivalent to E . Then $\chi_{\sigma,\tau} = \chi$ as equivalent extensions have the same coupling, so (σ,τ) lies in S_χ .

Now suppose that (σ,τ) lies in $\mathrm{AutQ} \times \mathrm{AutN}$. Then (σ,τ) lies in $\mathrm{Im}\,\Gamma$ if and only if there exists $\alpha : G \longrightarrow G$ such that the following diagram commutes.

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "i"] \arrow[d, "\tau"'] & G \arrow[r, "\pi"] \arrow[d, "\alpha"'] & Q \arrow[r] \arrow[d, "\sigma"'] & 1 \\
1 \arrow[r] & N \arrow[r, "i"] & G \arrow[r, "\pi"] & Q \arrow[r] & 1
\end{tikzcd}$$

But the existence of such an α is equivalent to the existence of an equivalence between the extensions

$$E : 1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow 1 \qquad \text{and}$$

$$E(\sigma,\tau) : 1 \longrightarrow N \xrightarrow{\tau^{-1}i} G \xrightarrow{\pi\sigma} Q \longrightarrow 1$$

of N by Q, so (σ,τ) lies in $\mathrm{Im}\,\Gamma$ if and only if $[E] = [E(\sigma,\tau)]$. Thus $\mathrm{Im}\,\Gamma = \mathrm{Stab}_{\mathrm{Aut}Q \times \mathrm{Aut}N}([E])$.

This gives us another way of expressing the sequence we obtained at the beginning of the section.

2.1.5 <u>Theorem</u> Let

$E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$ be an extension of N by Q with coupling χ, and let S_χ act on $\dfrac{Q}{N,\chi}$ as above. Then the following sequence is exact,

$$1 \longrightarrow C_{\mathrm{Aut}G}(G/N,N) \longrightarrow N_{\mathrm{Aut}G}(N) \xrightarrow{\Gamma} C_{S_\chi}([E]) \longrightarrow 1 .$$

<u>Proof</u> We substitute the expression for $\mathrm{Im}\,\Gamma$ obtained above into the sequence

$$1 \longrightarrow C_{\mathrm{Aut}G}(G/N,N) \longrightarrow N_{\mathrm{Aut}G}(N) \xrightarrow{\Gamma} \mathrm{Im}\,\Gamma \longrightarrow 1 .$$

2.1.6 <u>Corollary</u> Suppose that

$E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$

is an extension of N by Q with coupling χ, and that $H^2(Q,Z(N)) = 1$. Then

$$1 \longrightarrow Z^1(Q,Z(N)) \longrightarrow N_{\mathrm{Aut}G}(N) \xrightarrow{\Gamma} S_\chi \longrightarrow 1$$

is an exact sequence.

<u>Proof</u> 2.1.1 shows that $C_{\mathrm{Aut}G}(G/N,N) \cong Z^1(Q,Z(N))$. Since $H^2(Q,Z(N)) = 1$, 2.1.3 shows that $\dfrac{Q}{N,\chi}$ consists of just one element, $[E]$, and so $C_{S_\chi}([E]) = S_\chi$.

Wells in [11] provides an alternative statement of 2.1.5 and 2.1.6. He constructs a five term sequence

$$1 \longrightarrow Z^1(Q,Z(N)) \longrightarrow N_{\mathrm{Aut}G}(N) \xrightarrow{\Gamma} S_\chi \xrightarrow{\Delta} H^2(Q,Z(N))$$

which is exact in some sense although Δ defined below is only a set map and not a group homomorphism.

If $[F] \in \frac{Q}{N,\chi}$ let $\underline{F}$ be the corresponding element of $H^2(Q,Z(N))$.
Then if $(\sigma,\tau) \in S_\chi$ define $\Delta : S_\chi \longrightarrow H^2(Q,Z(N))$ by
$\Delta : (\sigma,\tau) \longrightarrow \{[\underline{E}] - [\underline{E(\sigma,\tau)}]\}$. Obviously Δ is not in general a group homomorphism, but $\mathrm{Ker}\Delta = \mathrm{Stab}_{S_\chi}([E]) = \mathrm{Im}\Gamma$ and this is the sense in which the sequence is exact.

2.1.6 also provides the key to Schmid's lifting theorem which we prove in section 2.3.

InnG is a subgroup of $N_{\mathrm{Aut}G}(N)$ so we now examine what happens to InnG under the action of Γ . Let $A/N = Z(Q)$ as before and let $U = \{(\mu_{dN}, d\rho) \mid d \in G\} \leq \mathrm{Aut}Q \times \mathrm{Aut}N$, where $\mu_{dN} \in \mathrm{Inn}Q$ and $\rho : G \longrightarrow \mathrm{Aut}N$ is defined as before.

2.1.7 <u>Lemma</u> Let

$$E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

be an extension of N by Q with coupling χ . Then the sequence

$$1 \longrightarrow (A \cap C_G(N))\mu \longrightarrow \mathrm{Inn}G \xrightarrow{\Gamma} U \longrightarrow 1$$

is exact.

<u>Proof</u> If μ_h is an element of InnG then μ_h lies in $\mathrm{Ker}\Gamma$ if and only if h centralises N and Q , that is if and only if $h \in C_G(N)$ and $hN \in Z(Q)$, that is if and only if $h \in C_G(N) \cap A$.
If $\mu_d \in \mathrm{Inn}G$ then $\mu_d\Gamma = (\mu_{dN}, \mu_d|_N) = (\mu_{dN}, d\rho)$ and so $\mathrm{Im}\Gamma = U$.

Combining this lemma with the sequence obtained in 2.1.5 gives us a description of $N_{OutG}(N) = N_{AutG}(N)/InnG$.

2.1.8 Lemma Let

$$E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

be an extension of N by Q with coupling χ . Then the following sequence is exact

$$1 \longrightarrow C_{AutG}(G/N,N)/(A \cap C_G(N))\mu \longrightarrow N_{OutG}(N) \xrightarrow{\Gamma} C_{S_\chi}([E])/U \longrightarrow 1 .$$

Proof Apply the snake lemma to the sequences obtained in 2.1.5 and 2.1.7 .

2.1.2 gives an immediate corollary to this.

2.1.9 Corollary Suppose that the conditions of 2.1.8 hold and that $C_G(N) = Z(N)$. Then there is an exact sequence

$$1 \longrightarrow H^1(G/N,Z(N)) \longrightarrow N_{OutG}(N) \xrightarrow{\Gamma} C_{S_\chi}([E])/U \longrightarrow 1 .$$

Proof Use 2.1.2 to substitute for $C_{AutG}(G/N,N)/(A \cap C_G(N))\mu$ in the sequence obtained in the previous lemma.

Section 2.2

In this section we consider central automorphisms of a group. We use the results of the previous section to obtain exact sequences described by Robinson in [7] , and then use these sequences to obtain information about automorphisms of a particular class of FC groups which contains the finitely generated nilpotent groups of Hirsch length one.

An extension

$E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$

of a group N by a group Q is called central if N lies inside $Z(G)$. If E is central then $G\rho = 1$ and if χ is the coupling associated with E then $Q\chi = 1$ because χ is defined by the diagram

$$\begin{array}{ccc} G & \xrightarrow{\rho} & \mathrm{Aut}N \\ \downarrow & & \downarrow \\ Q & \xrightarrow{\chi} & \mathrm{Out}N \end{array}$$

Thus $S_\chi = C_{\mathrm{Aut}Q \times \mathrm{Aut}N}(\chi) = C_{\mathrm{Aut}Q \times \mathrm{Aut}N}(1) = \mathrm{Aut}Q \times \mathrm{Aut}N$.

The following lemma is due to Robinson [7] . Q_{ab} denotes Q factored by its derived group.

2.2.1 <u>Lemma</u>(Robinson) Let $E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$ be a central extension of N by Q . Then there is an exact sequence

$$1 \longrightarrow \mathrm{Hom}(Q_{ab}, N) \longrightarrow N_{\mathrm{Aut}G}(N) \longrightarrow C_{\mathrm{Aut}Q \times \mathrm{Aut}N}([E]) \longrightarrow 1$$

<u>Proof</u> We apply 2.1.5, and so it suffices to show that $C_{\mathrm{Aut}G}(G/N, N)$ is isomorphic to $\mathrm{Hom}(Q_{ab}, N)$. But 2.1.1 shows that

$C_{AutG}(G/N,N)$ is isomorphic to $Z^1(G/N,Z(N))$, which can be identified with $Der(Q,Z(N))$, the group of derivations of Q in $Z(N)$ (see e.g. [5]) . Since Q acts trivially on N , which is just $Z(N)$, $Der(Q,Z(N))$ is equal to $Hom(Q_{ab},N)$. For if $\alpha \in Der(Q,Z(N))$ then $(q.r)\alpha = (q)\alpha^r.(r)\alpha = (q)\alpha.(r)\alpha$ for all q,r in Q , so α defines a homomorphism from Q to $Z(N)$. However N is abelian so any element of $Hom(Q,N)$ must act trivially on Q' , and so $Hom(Q,N)$ can be identified with $Hom(Q_{ab},N)$.

Now we consider the group U that arose in our description of $InnG$ in section 2.1 . $U = \{(\mu_{dN}, d\rho) \mid d \in G\} = \{(\mu_{dN}, 1) \mid d \in G\}$ as $G\rho = 1$, so U is the subgroup $InnQ \times 1$ of $AutQ \times AutN$. Since $C_G(N) = G$. $A \cap C_G(N) = A$ and the exact sequence of 2.1.7 becomes $1 \longrightarrow (A)\mu \longrightarrow InnG \longrightarrow InnQ \times 1 \longrightarrow 1$ in this case. U is a subgroup of $Stab_{AutQ \times AutN}([E])$ but the definition of U is now independent of $[E]$ and so U must act trivially on $\frac{Q}{N,\chi}$. As $InnQ \times 1$ acts trivially on $\frac{Q}{N,\chi}$ we get an action of $AutQ \times AutN/InnQ \times 1 = OutQ \times AutN$ on $\frac{Q}{N,\chi}$.

2.2.2 <u>Lemma</u> (Robinson) Let

$$E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

be a central extension of N by Q . Then there is an exact sequence of groups

$$1 \longrightarrow N \longrightarrow Z(G) \longrightarrow Z(Q) \xrightarrow{H} Hom(Q_{ab},N) \longrightarrow N_{OutG}(N) \longrightarrow C_{OutN \times AutQ}([E]) \longrightarrow 1 \ .$$

<u>Proof</u> We examine 2.1.8 . In this case

$C_{S_\chi}([E])/U = C_{\mathrm{AutQ} \times \mathrm{AutN}}([E])/\mathrm{InnQ} \times 1 \cong C_{\mathrm{OutQ} \times \mathrm{AutN}}([E])$.

Let A be a subgroup of G containing N such that $A/N = Z(Q)$.
We have a map $H : Z(Q) \longrightarrow (A)\mu$ defined by $H : qN \longrightarrow \mu_q \in (A)\mu$ for any qN in Q . The kernel of H is the subgroup $Z(G)/N$ of $Z(Q)$ and so we get an exact sequence

$$1 \longrightarrow N \longrightarrow Z(G) \longrightarrow Z(Q) \xrightarrow{H} (A)\mu \longrightarrow 1 .$$

In this case the exact sequence of 2.1.8 becomes

$$1 \longrightarrow C_{\mathrm{AutG}}(G/N,N)/(A)\mu \longrightarrow N_{\mathrm{OutG}}(N) \longrightarrow C_{\mathrm{OutQ} \times \mathrm{AutN}}([E]) \longrightarrow 1$$

since $A \cap C_G(N) = A$, $S_\chi = \mathrm{AutQ} \times \mathrm{AutN}$, and $U = \mathrm{InnQ} \times 1$ acts trivially on $\frac{Q}{N,\chi}$, so we may identify $C_{S_\chi}([E])/U$ and $C_{\mathrm{OutQ} \times \mathrm{AutN}}([E])$. Identifying $C_{\mathrm{AutG}}(G/N,N)$ and $\mathrm{Hom}(Q_{ab},Z(G))$, and combining the two sequences gives the result.

2.2.3 <u>Corollary</u> Let G be a group and let $Q = G/Z(G)$. Let E be the element of $\frac{Q}{Z(G),1}$ corresponding to G . There is an exact sequence

$$1 \longrightarrow Z(Q) \longrightarrow \mathrm{Hom}(Q_{ab},Z(G)) \longrightarrow \mathrm{OutG} \longrightarrow C_{\mathrm{OutQ} \times \mathrm{AutN}}([E]) \longrightarrow 1$$

<u>Proof</u> Apply the previous result with $N = Z(G)$. $Z(G)$ is characteristic in G so $N_{\mathrm{OutG}}(Z(G)) = \mathrm{OutG}$.

We have discussed so far the action of S_χ on $\frac{Q}{N,\chi}$. If $\frac{Q}{N,\chi}$ is non-empty this induces some action of S_χ on $H^2(Q,Z(N))$. When N is abelian and a trivial Q module we have seen that $S_\chi = \mathrm{AutQ} \times \mathrm{AutN}$; in this case the action of S_χ on $H^2(Q,N)$ arises in another way.

For $H^i(Q,N)$ is an $\mathrm{Aut}Q \times \mathrm{Aut}N$ module for any $i \geqslant 0$ as follows. Applying the functor $H^i(Q,\ )$ to any $\gamma \in \mathrm{Aut}N$ yields $\gamma^* : H^i(Q,N) \longrightarrow H^i(Q,N)$. Any $\delta \in \mathrm{Aut}Q$ induces a natural transformation called conjugation $c^\delta : H^i(Q,M) \longrightarrow H^i(Q,M^\delta)$ for any Q-module M, where M^δ is the abelian group M with Q action defined by $m \circ q = m(q)\delta^{-1}$ for any q in Q and m in M. (See [5]). Since N is a trivial Q-module $N = N^\delta$ and c^δ defines an action of $\mathrm{Aut}Q$ on $H^i(Q,N)$; the action is trivial for any $\delta \in \mathrm{Inn}Q$. The actions of $\mathrm{Aut}Q$ and $\mathrm{Aut}N$ commute so we have actions of $\mathrm{Aut}Q \times \mathrm{Aut}N$ and $\mathrm{Out}Q \times \mathrm{Aut}N$ on $H^i(Q,N)$, and we may check that the action this defines on $H^2(Q,N)$ is just that arising from the action of $\mathrm{Aut}Q \times \mathrm{Aut}N$ on $\dfrac{Q}{N,1}$ defined above.

We shall now consider what this tells us about FC groups. We recall that an FC group is one in which every element has finitely many conjugates. In a finitely generated FC group G the centre has finite index so is finitely generated, and is abelian so contains some free abelian subgroup C of finite index. The rank of C is just the Hirsch length of $Z(G)$. We apply our previous results to get the following lemma.

2.2.4 <u>Lemma</u> Let G be a finitely generated FC group and let C be a free abelian subgroup of $Z(G)$ of finite index in G. Let $S = G/C$ and let $E : 1 \longrightarrow C \longrightarrow G \longrightarrow S \longrightarrow 1$ denote the extension corresponding to G. Then

$N_{\mathrm{Aut}G}(C) \geqslant C_{\mathrm{Aut}S \times \mathrm{Aut}C}([E])$ and

$N_{\mathrm{Out}G}(C) \geqslant C_{\mathrm{Out}S \times \mathrm{Aut}C}([E])$.

<u>Proof</u> The theorem follows from 2.2.1 and 2.2.2 since, as S is finite and C is free abelian, $\mathrm{Hom}(S_{ab},C)$ is trivial.

The rest of this section is concerned with analysing the action of $\mathrm{Aut}S \times \mathrm{Aut}C$ on $H^2(S,C)$ to enable us to obtain alternative expressions of the result of the previous lemma.

Since C is torsion free C can be identified with some $\mathbb{Z}S$ submodule of $C \otimes_{\mathbb{Z}} \mathbb{Q}$ and if $\tilde{C} = C\otimes_{\mathbb{Z}}\mathbb{Q}/C$ then $\tilde{C}$ is a trivial $\mathbb{Z}S$ module. Since $\mathbb{Q}$ is $\mathbb{Z}$ flat as a $\mathbb{Z}$ module we have $H^i(S,C\otimes_{\mathbb{Z}}\mathbb{Q}) = H^i(S,C)\otimes_{\mathbb{Z}}\mathbb{Q}$ for all i (see e.g. [5] p.233) and since S is finite $H^i(S,C)$ is a torsion module ([5] p.91) so $0 = H^i(S,C)\otimes_{\mathbb{Z}}\mathbb{Q} = H^i(S,C\otimes_{\mathbb{Z}}\mathbb{Q})$. Applying the long exact sequence of cohomology to the exact sequence $0 \longrightarrow C \longrightarrow C\otimes_{\mathbb{Z}}\mathbb{Q} \rightarrow \tilde{C} \longrightarrow 0$ of (trivial) $\mathbb{Z}S$ modules yields the exact sequence $0 = H^1(S,C\otimes_{\mathbb{Z}}\mathbb{Q}) \longrightarrow H^1(S,\tilde{C}) \xrightarrow{d} H^2(S,C) \longrightarrow H^2(S,C\otimes_{\mathbb{Z}}\mathbb{Q}) = 0$ where d is the connecting homomorphism.

$H^1(S,\tilde{C})$ is naturally isomorphic to $\mathrm{Der}(S,\tilde{C})/\mathrm{Ider}(S,\tilde{C})$. Since S acts trivially on $\tilde{C}$, $\mathrm{Der}(S,\tilde{C})$ is just $\mathrm{Hom}_{\mathbb{Z}}(S,\tilde{C})$ and $\mathrm{Ider}(S,\tilde{C})$ is trivial so $H^1(S,\tilde{C})$ is naturally isomorphic to $\mathrm{Hom}_{\mathbb{Z}}(S,\tilde{C})$ which can be identified with $\mathrm{Hom}_{\mathbb{Z}}(S_{ab},\tilde{C})$

As S acts trivially on $\tilde{C}$ we have actions of $\mathrm{Aut}S \times \mathrm{Aut}\tilde{C}$ and $\mathrm{Out}S \times \mathrm{Aut}\tilde{C}$ on $H^1(S,\tilde{C})$ as before. Any element of $\mathrm{Aut}C$ induces an automorphism of $C\otimes_{\mathbb{Z}}\mathbb{Q}$ and hence of $\tilde{C}$ so we may regard $\mathrm{Aut}C$ as a subgroup of $\mathrm{Aut}\tilde{C}$ and we have an action of $\mathrm{Aut}S \times \mathrm{Aut}C$ and $\mathrm{Out}S \times \mathrm{Aut}C$ on $H^1(S,\tilde{C})$ and thus on $\mathrm{Hom}_{\mathbb{Z}}(S_{ab},\tilde{C})$. One may check that if $\theta \in \mathrm{Hom}(S_{ab},\tilde{C})$ and $(\sigma,\jmath) \in \mathrm{Aut}S \times \mathrm{Aut}C$ then $\theta(\sigma,\jmath)$ is defined so as to make the following diagram commute.

$$\begin{array}{ccc} S_{ab} & \xrightarrow{\sigma} & S_{ab} \\ \theta \downarrow & & \downarrow \theta(\sigma, J) \\ \tilde{C} & \xrightarrow[J]{} & \tilde{C} \end{array} \quad .$$

Now given any $\eta \in \mathrm{AutS} \times \mathrm{AutC}$ it follows from our construction and naturality that the following diagram commutes

$$\begin{array}{ccccc} H^2(S,C) & \overset{d}{\cong} & H^1(S,\tilde{C}) & \cong & \mathrm{Hom}\,(S_{ab},\tilde{C}) \\ \eta \downarrow & & \eta \downarrow & & \eta \downarrow \\ H^2(S,C) & \overset{d}{\cong} & H^1(S,\tilde{C}) & \cong & \mathrm{Hom}\,(S_{ab},\tilde{C}) \end{array} \quad .$$

We have thus proved the following theorem

2.2.5 __Theorem__ Let G be a finitely generated FC group and let C be a free abelian subgroup of $Z(G)$ of maximal rank. Let $S = G/C$ and let $E : 1 \longrightarrow C \longrightarrow G \longrightarrow S \longrightarrow 1$ be the extension of C by S corresponding to G. Then

$N_{\mathrm{AutG}}(C) \cong C_{\mathrm{AutS} \times \mathrm{AutC}}(\pi)$ and

$N_{\mathrm{OutG}}(C) \cong C_{\mathrm{OutS} \times \mathrm{AutC}}(\pi)$ where π is the element of $\mathrm{Hom}_{\mathbb{Z}}(S_{ab},\tilde{C})$ corresponding to $[E]$.

This result could be applied to investigate the structure of OutG in general; to conclude this section we examine its consequences when $Z(G)$ has Hirsch length one. In this case C is infinite cyclic and $\tilde{C} \cong \mathbb{Q}/\mathbb{Z}$. Then as S_{ab} is finite we can show, by choosing a generating set for S_{ab} and using it to define a generating set for $\mathrm{Hom}_{\mathbb{Z}}(S_{ab},\tilde{C})$, that there exists an isomorphism $\alpha : \mathrm{Hom}(S_{ab},\tilde{C}) \longrightarrow S_{ab}$. α is not necessarily natural, and in general there does not exist a natural isomorphism between $\mathrm{Hom}_{\mathbb{Z}}(S_{ab},\tilde{C})$ and S_{ab}. However we can use α to define an action of $\mathrm{AutS} \times \mathrm{AutC}$ and $\mathrm{OutS} \times \mathrm{AutC}$ on S_{ab}; if $\zeta \in \mathrm{AutS} \times \mathrm{AutC}$ we define the action of ζ on S_{ab} so as to make the following diagram commute

$$\begin{tikzcd} \mathrm{Hom}(S_{ab},\tilde{C}) \arrow[r, "\alpha"] \arrow[d, "\zeta"'] & S_{ab} \arrow[d, "\zeta"] \\ \mathrm{Hom}(S_{ab},\tilde{C}) \arrow[r, "\alpha"] & S_{ab} \end{tikzcd}$$

Now C is infinite cyclic so $\mathrm{Aut}C$ has order two and if β is a generator of $\mathrm{Aut}C$ an examination of the commutative diagrams demonstrates that $(1,\beta)$ acts on S_{ab} by inverting every element. If $(\mu,1) \in \mathrm{Aut}S \times \mathrm{Aut}C$ for some μ in $\mathrm{Aut}S$ then we may verify that $(\mu,1)$ acts on S_{ab} as the transpose, with respect to the generating set we chose for S_{ab}, of μ^{-1}. Thus in particular the action of $(\mu,1)$ on S_{ab} may not be induced on S_{ab} by the action on S of any automorphism of S. Combining this with 2.2.5 yields

2.2.6 <u>Theorem</u> Let G be a finitely generated FC group whose centre has Hirsch length one, and C some infinite cyclic subgroup of $Z(G)$. Let $S = G/C$ and let $E : 1 \longrightarrow C \longrightarrow G \longrightarrow S \longrightarrow 1$ be the extension of C by S corresponding to G. Then $N_{\mathrm{Out}G}(C)$ is non-trivial if and only if $C_{\mathrm{Out}S \times \langle\beta\rangle}(u)$ is non-trivial where $u \in S_{ab}$ corresponds to $[E]$ under the isomorphism of S_{ab} with $H^2(S,C)$ which defines the action of $\mathrm{Out}S$ on S_{ab}.

The following corollary is the reason for proving the theorem.

2.2.7 <u>Corollary</u> Let G be a group and let C be an infinite cyclic subgroup of $Z(G)$ such that $S = G/C$ is finite. If S admits a non-inner automorphism which centralises S_{ab} then G admits a non-inner automorphism.

<u>Proof</u> Let $E : 1 \longrightarrow C \longrightarrow G \longrightarrow S \longrightarrow 1$ be the extension of C by S corresponding to G, and let $\bar{\nu} = \nu.\mathrm{Inn}S \neq 1$ be an element of $\mathrm{Out}S$ centralising S_{ab}. Then in the action of $\mathrm{Out}S \times \mathrm{Aut}C$ defined on S_{ab} via $H^2(S,C)$, $(\bar{\nu}, 1_C)$ centralises any element of S_{ab}. So $(\bar{\nu}, 1_C)$ is a non-trivial element of $N_{\mathrm{Out}S \times \mathrm{Aut}C}(u)$ where u is the element of S_{ab} corresponding to $[E]$, and the result follows from 2.2.6.

If G is a finitely generated nilpotent group of Hirsch length one then $Z(G)$ is infinite so also has Hirsch length one and $G/Z(G)$ is finite. Thus to find a non-inner automorphism of G it is sufficient to find an infinite cyclic subgroup C of $Z(G)$ such that G/C admits a non-inner automorphism centralising its derived quotient. Unfortunately many finite nilpotent groups fail to admit a non-inner automorphism of this type; examples include the extraspecial p-groups. Nevertheless one could approach the problem of finding a non-inner automorphism of G by trying to classify all finite nilpotent groups which lack this type of non-inner automorphism although we shall not attempt this here.

Section 2.3

In proving theorems about automorphisms of groups one of the most difficult problems is to find ways of using induction. Schmid [9] overcomes this in his proof of Gaschutz' theorem which we give in this section; it depends on a lifting theorem which we now prove.

If N is a normal subgroup of a group G denote by ${}_GL_N$ the group of automorphisms of N which lift to automorphisms of G; formally ${}_GL_N = \{ \alpha \in \mathrm{Aut}N \mid \exists \beta \in \mathrm{Aut}G \text{ with } \beta|_N = \alpha \}$.
Let Q be G/N. We have established a map $\Gamma : \mathrm{Aut}G \longrightarrow \mathrm{Aut}Q \times \mathrm{Aut}N$. Let π be the projection from $\mathrm{Aut}Q \times \mathrm{Aut}N$ onto $\mathrm{Aut}N$. Then if $\alpha \in \mathrm{Aut}N$ there will be an automorphism β of G inducing α on N if and only if $\alpha \in \mathrm{Im}(\Gamma\pi)$, and so ${}_GL_N = \mathrm{Im}(\Gamma\pi)$.

2.3.1 <u>Theorem</u> (Schmid) Suppose that

$$E : 1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1$$

is an extension of N by Q with coupling χ, such that $C_G(N) = Z(N)$ and $H^2(Q,Z(N)) = 1$. Then ${}_GL_N = N_{\mathrm{Aut}N}(G\rho)$.

<u>Proof</u> Since $H^2(Q,Z(N)) = 1$ we know by 2.1.6 that $\mathrm{Im}\Gamma = S\chi$. Thus $\alpha \in {}_GL_N = \mathrm{Im}(\Gamma\pi)$ if and only if there exists $\jmath \in \mathrm{Aut}Q$ such that $(\jmath,\alpha) \in S\chi = C_{\mathrm{Aut}Q \times \mathrm{Aut}N}(\chi)$, that is if and only if there exists $\jmath \in \mathrm{Aut}Q$ making the following diagram commute.

$$\begin{array}{ccc} Q & \xrightarrow{\chi} & \mathrm{Out}N \\ {\scriptstyle \jmath}\downarrow & & \downarrow{\scriptstyle \mu_{\bar\alpha}} \\ Q & \xrightarrow[\chi]{} & \mathrm{Out}N \end{array}$$

Now $C_Q(N) = Z(N)$ so χ is injective and $\mathrm{Im}\chi = \overline{G\rho}$, the image of $G\rho$ in OutN. So we have a diagram

$$\begin{array}{ccc} Q & \xrightarrow{\chi} & \overline{G\rho} \\ & & \downarrow \mu_{\bar\alpha} \\ Q & \xrightarrow{\chi} & \mathrm{OutN} \end{array}$$

and a $\mathcal{J}$ will exist as required if and only if

$\overline{G\rho}.\mu_{\bar\alpha} = Q\chi = \overline{G\rho}$ that is if and only if $(G\rho)^{\alpha} = G\rho$, that is if and only if $\alpha \in N_{\mathrm{AutN}}(G\rho)$,, since InnN lies inside $G\rho$.

Gaschütz showed in [3,7] that any finite p-group of order at least p has an outer automorphism of order p, which settled a long standing conjecture. The inductive element in his proof comes from a powerful cohomological lemma due to Gaschütz, see e.g. [5].

2.3.2 Lemma Let Q be a finite p-group, and let N be an Q-module which is also a p-group. If $H^1(Q,N) = 0$ then $H^k(S,N) = 0$ for all subgroups S of Q and for all $k \geqslant 1$.

On the other hand Schmid's proof uses only the cohomology of cyclic groups. We recall that if $A = \langle a \rangle$ is a finite cyclic group and B is an A module then $H^1(A,B) = \mathrm{Ker}\mathcal{J}/[a,B]$ and $H^2(A,B) = C_B(a)/\mathrm{Im}\,\mathcal{J}$ where $\mathcal{J} : B \longrightarrow B$ is the trace map. In particular if B is finite $|H^1(A,B)| = |H^2(A,B)|$, which demonstrates a special case of 2.3.2 when $H^1(A,B) = 0$.

In fact Schmid proves a slightly stronger result than that of Gaschutz. Any inner automorphism of a group G centralises the centre of G so InnG is a subgroup of $C_{\mathrm{AutG}}(Z(G))$, and we may define $C_{\mathrm{OutG}}(Z(G))$ to be $C_{\mathrm{AutG}}(Z(G))/\mathrm{InnG}$.

2.3.3 Theorem(Schmid) Let G be a finite non-abelian p-group. Then p divides the order of $C_{OutG}(Z(G))$.

Proof We shall use induction on $|G|$. Suppose that G is a finite non-abelian p-group and that the theorem holds for all finite non-abelian p-groups with smaller order than that of G . Let N be a maximal subgroup of G which contains $Z(G)$; as $G/Z(G)$ is non-trivial we can always find such an N . $C_G(N) = Z(N)$ as otherwise we would have $G = \langle x,N \rangle$ for some $x \in C_G(N)$ and x would be in $Z(G)$ contradicting our choice of N . If $\rho : G \longrightarrow AutN$ as before then $Ker\rho = C_G(N) = Z(N)$ so $|G\rho| = |G:Z(N)|$. $InnN$ is a subgroup of $G\rho$ and so $|G\rho/InnN| = |G:Z(N)|/|N:Z(N)| = p$.

If $H^1(G/N,Z(N)) \neq 1$ then 2.1.2 shows that $C_{AutG}(G/N,N)$ does not lie in $InnG$. $C_{AutG}(G/N,N)$ centralises a series in the p-group G so is a p-group, and a subgroup of $C_{AutG}(Z(G))$ since $Z(G) \leq N$. Thus $C_{AutG}(G/N,N).InnG/InnG$ is a non-trivial p-subgroup of $C_{OutG}(Z(G)) = C_{AutG}(Z(G))/InnG$ and the result follows.

Thus we may assume that $H^1(G/N,Z(N)) = 1$. There are two possibilities to consider.

Case 1 There exists a maximal subgroup N of G which contains $Z(G)$ and is not abelian.

In this case our induction hypothesis allows us to assume that $p \,\Big|\, |C_{OutN}(Z(N))|$. $C_{OutN}(Z(N))$ is normal in $OutN$ and so $G\rho/InnN$ which is a p-group acts on $C_{OutN}(Z(N))$ and must centralise some subgroup $A/InnN$ of $C_{OutN}(Z(N))$ with $A/InnN$ of order p . Thus $[G\rho,A] \leq InnN \leq G\rho$ and so $A \leq N_{AutN}(G\rho)$.

Now we can use the lifting theorem. G/N is cyclic and $H^1(G/N,Z(N))$ is zero so $H^2(G/N,Z(N))$ is zero. $C_G(N) = Z(N)$ and A is a subgroup of $N_{AutN}(G\rho)$ so 2.3.1 shows that there exists a subgroup B of AutG such that B normalises N and $B|_N = A$. A centralises $Z(N)$ so B centralises $Z(G)$ which is a subgroup of $Z(N)$. Considering the proof of 2.3.1 we see that in this case $\overline{G\rho}$ has order p and so $\mu_{\bar{\alpha}}$ acts on it as the identity and thus B acts on G/N as the identity. B acts on N as the p-group A so B is a p-group.

If B lies in InnG then $B \cong D/Z(G)$ for some subgroup D of G, and $B|_N = D\rho = A$ so A/InnN is a non-trivial subgroup of $G\rho/\mathrm{InnN} \cap C_{OutN}(Z(N))$. $G\rho/\mathrm{InnN}$ has order p so this implies that $G\rho/\mathrm{InnN}$ is a subgroup of $C_{OutN}(Z(N))$ and that $G\rho$ is a subgroup of $C_{AutN}(Z(N))$. But this is just another way of saying that $Z(N)$ centralises G, and so as $Z(G) \leqslant Z(N)$ we must have $Z(N)$ and $Z(G)$ equal. However if this happens then G/N acts trivially on $Z(N)$ and the remarks after 2.3.2 show that $H^1(G/N,Z(N))$ cannot be zero. But we have shown that we can assume that $H^1(G/N,Z(N))$ is zero, and so have a contradiction to our hypothesis that B lies in InnG. Thus $B.\mathrm{InnG}/\mathrm{InnG}$ is a non-trivial p-subgroup of $C_{OutN}(Z(G))$ and the result follows.

Case 2 All maximal subgroups of G which contain $Z(G)$ are abelian.

If all maximal subgroups of G which contain $Z(G)$ are cyclic then I claim that G is the quaternion group of order 8. If we can show that G has no subgroup isomorphic to $C_p \times C_p$ then this follows from a well known result of P.Hall, see e.g. [4]. But if G contains a subgroup isomorphic to $C_p \times C_p$ then G

contains a subgroup H isomorphic to $C_p \times C_p$ such that $H \cap Z(G) \neq 1$; then $\langle H, Z(G) \rangle$ is abelian and non-cyclic and contains $Z(G)$ so lies in some maximal subgroup N which contains $Z(G)$ and is not cyclic, which is impossible if all maximal subgroups of $Z(G)$ are cyclic. The quaternion group of order 8 has automorphism group isomorphic to Σ_4 and outer isomorphism group isomorphic to Σ_3 ; any non- inner automorphism must fix its centre as it has order 2 . (This is explained in more detail in chapter 4). Thus the theorem holds if all maximal subgroups of G which contain $Z(G)$ are cyclic , so we may assume that there exists one, N say, which is abelian but not cyclic. $G/Z(G)$ is not cyclic so we may assume that there exists another maximal subgroup M of G which contains $Z(G)$ and is abelian; then $G = \langle M, N \rangle$. $M \cap N$ centralises both M and N so $M \cap N$ is a subgroup of $Z(G)$; G' is equal to $[M,N]$ which is a subgroup of $M \cap N$ so $G' \leq Z(G)$. Since G is not abelian $|G:Z(G)| \geq p^2 = |G:M \cap N|$ and so $M \cap N = Z(G)$. Let $G = \langle y, N \rangle$ and $N = \langle x, Z(G) \rangle$ for some $y \in G$ and $x \in N$.

Now $H^1(G/N, Z(N)) = 1$ so $H^2(G/N, Z(N)) = 1$ as G/N is cyclic, and we do some calculations using the formulae given after 2.3.2 . As $H^2(G/N, Z(N)) = 1$ $N\mathcal{J} = C_{Z(N)}(y) = C_N(y) = Z(G)$ where $\mathcal{J}$ is the trace map and $n\mathcal{J} = n^{1+y+ \cdots +y^{p-1}}$ for all n in N . Thus $Z(G) = N\mathcal{J} = \langle x\mathcal{J}, Z(G)\mathcal{J} \rangle$. Since $g\mathcal{J} = g^p$ for all g in $Z(G)$ $Z(G) = \langle x\mathcal{J}, \mho_1(Z(G)) \rangle = \langle x\mathcal{J} \rangle$ as $\mho_1(Z(G))$ is just the Frattini subgroup of $Z(G)$. Thus $Z(G)$ is cyclic. Since N is not cyclic x may be chosen so that $x^p = 1$. x and y do not commute so let $x^y = xu$ for some u in $Z(G)$. Then $u^p = x^{-p}.x^{p^y} = 1$. $x\mathcal{J} = x^{1+y- \cdots +y^{p-1}} = x.xu. \ldots .xu^{p-1} = x^p.u^{\frac{1}{2}p(p-1)} = u^{\frac{1}{2}p(p-1)}$.

If p is not equal to 2 then $x\vartheta = u^{p(p-1)/2}$ and $x\vartheta$ lies in $\mathcal{U}_1(Z(G))$ which is impossible as $Z(G)$ is generated by $x\vartheta$. Thus $p = 2$ and $Z(G)$ is generated by $x\vartheta = u$ so $Z(G)$ has order 2 , and G has order 8 . Since G is non-abelian and has a non-cyclic abelian subgroup G must be isomorphic to the dihedral group of order 8 . This group is isomorphic to its own automorphism group and its outer automorphism group has order 2; any non-inner automorphism must centralise the centre which has order 2 . Thus the theorem is proved.

2.3.4 <u>Corollary</u> Let G be a finite p-group of order at least p . Then G admits a non-inner automorphism of p-power order.

<u>Proof</u> If G is not abelian then the result follows from the previous theorem . If G is abelian all automorphisms are non-inner. Let N be a maximal subgroup of G , and let $G = \langle a, N \rangle$ for some a in G . As G has order at least p we may pick an element x of N of order p. The map $\gamma : a \longrightarrow ax$, $\gamma : n \longrightarrow n$ for all n in N is an automorphism of G of order p and is not inner .

2.3.5 <u>Corollary</u> Any finite nilpotent group of order at least three admits a non-inner automorphism.

<u>Proof</u> If G is a finite nilpotent group of order at least three then G can be expressed as $D \times E$ where D is a p-group of order at least three for some prime p and E is a p' group. If D is not of order p then the previous result shows that D has a non-inner automorphism; if D has order p then the map $\gamma : x \longrightarrow x^2$ for all x in D is a non-inner automorphism of D . In either case

we can write down a non-inner automorphism α of G defined by $\alpha|_D$ is any non-inner automorphism of D and $\alpha|_E = 1_E$.

Schmid has also shown that if G is a p-group which is not extraspecial or elementary abelian then OutG has a non-trivial normal p-subgroup which can be described fairly explicitly.

Chapter Three Reducing the problem to a question about p-groups

It is now time to attack the problem of finding non-inner automorphisms of finitely generated nilpotent groups of Hirsch length one. Our aim in this chapter is to show how to reduce the problem to a question about automorphisms of finite p-groups. After introducing some notation we produce in section 1 a two part criterion for non-inner automorphisms to exist. We use this criterion in section 2 to deduce that certain classes of finitely generated nilpotent groups admit non-inner automorphisms, in particular those of nilpotency class two. The rest of this essay will be about finite p-groups, and the way they arise is explained in section 3, which also contains some further reductions of the problem.

Throughout this chapter G will denote a finitely generated nilpotent group of Hirsch length one and T its torsion subgroup. T is normal in G and G/T is infinite cyclic. Denote by zT some generator of G/T and let $\phi = z\rho \in \mathrm{Aut}T$, where $\rho : G \longrightarrow \mathrm{Aut}T$. Then $G\rho$ is the subgroup of $\mathrm{Aut}T$ generated by ϕ and $\mathrm{Inn}T$.

Conversely given U a finite nilpotent group and ψ an automorphism of U which acts nilpotently on U the group $H = U \rtimes \langle y \rangle$, where y acts on U as ψ, is a finitely generated nilpotent group with torsion subgroup U. H/U is an infinite cyclic group so H has Hirsch length one and if $\rho : H \longrightarrow \mathrm{Aut}U$ then $y\rho = \psi$.

We now introduce some notation which will be used frequently. Given $uZ(T) \in T/Z(T)$ we denote by μ_u the element of InnT which acts as conjugation by u . If α is an element of AutT then we have $\alpha^{-1}\mu_u\alpha = \mu_{u\alpha}$. We let $\bar{\alpha}$ be the image of α in OutT . The group generated by ϕ is cyclic so $\langle\phi\rangle \cap$ InnT is a cyclic group generated by $\phi^m = \mu_c$ say for some integer m and some $cZ(T)$ in $T/Z(T)$. Thus the group generated by $\bar{\phi}$ is cyclic of order m . We have a commutative diagram

$$\begin{array}{ccccc} G & \xrightarrow{\rho} & \langle \phi , \mathrm{InnT} \rangle & \longrightarrow & \mathrm{AutT} \\ \downarrow & & \downarrow & & \\ G/T & \xrightarrow[\chi]{} & \langle \bar{\phi} \rangle & & \end{array}$$

and so $\langle\bar{\phi}\rangle$ is just $(G/T)\chi$ where $\chi : G/T \longrightarrow$ OutT is the coupling associated with the extension

$E : 1 \rightarrow T \rightarrow G \rightarrow G/T \rightarrow 1$.

Thus m is independent of our choice of z .

The element μ_c of InnT will play an important part in what follows. Let $V = \langle c,Z(T)\rangle$. Then V is abelian. For any $t \in T$ we have $t^{c\phi} = ((t\phi^{-1})^c)\phi = t\phi^{-1}\phi^m\phi = t\phi^m = t^c$ so $c^{-1}\phi.c \in Z(T)$ and V is ϕ-invariant. Define $\alpha : V \longrightarrow V$ by $\alpha : v \longrightarrow v^{-1}\phi.v$ for all $v \in V$. Since V is abelian α is a group homomorphism, and $V\alpha = [\phi,\langle c,Z(T)\rangle] \leq Z(T)$. We shall show by routine calculation that $V\alpha$ is independent of our choice of z. Suppose $\psi = \phi^e\mu_t$, where $e \in \{1,-1\}$ and $t \in T$. Then $\psi^m = (\phi^e\mu_t)^m = \phi^{em}\mu_n = \mu_{c^e.n}$ where $n = t\phi^{e(m-1)}.t\phi^{e(m-2)}\ldots t\phi^e.t$. Notice that $n\phi^e = t\phi^{em}.t\phi^{e(m-1)}\ldots t\phi^e = t^{c^e}.n.t^{-1}$. Let $W = \langle c^e n,Z(T)\rangle$, and let $\beta : W \longrightarrow W$ be given by $\beta : w \longrightarrow w^{-1}\psi.w$ for all $w \in W$. Then if $x \in Z(T)$, $x\beta = x^{-1}\psi.x = x^{-1}\phi^e\mu_t.x = x^{-1}\phi^e.x \in Z(T)\alpha$, and we can deduce that $Z(T)\beta = Z(T)\alpha$. Thus $W\beta = \langle (c^e n)\beta, Z(T)\alpha\rangle$.

$$\begin{aligned} \text{Now}\quad (c^e n)\beta &= (c^e n)^{-1}\psi.c^e n = (n^{-1}c^{-e})\phi^e\mu_t.c^e n \\ &= \{tn^{-1}(t^{c^e})^{-1}.(c^{-e})\phi^e\}^t\, c^e n = t^{-1}tn^{-1}c^{-e}t^{-1}c^e.(c^{-e})\phi^e.tc^e n \\ &= c^e.(c^{-e})\phi^e \end{aligned}$$

since $c^e.(c^{-e})\phi^e \in Z(T)$, and so $W\beta = V\alpha$.

Section 3.1

We are going to describe AutG and InnG in terms of exact sequences, in the manner of chapter 2, and to use these sequences to obtain a description of NilG . Although we could use the methods we used there we shall instead obtain these sequences by direct calculation, both for variety and because the explicit formulation of these results will be needed later. At the end of the section we give some examples.

T is a characteristic subgroup of G and so we have maps

$\mathrm{AutG} = N_{\mathrm{AutG}}(T) \xrightarrow{\Gamma} \mathrm{AutG/T} \times \mathrm{AutT} \xrightarrow{\pi_T} \mathrm{AutT}$

as defined in 2.1. We shall denote $\Gamma\pi_T$ by Δ . We also have maps

$\mathrm{AutG} = N_{\mathrm{AutG}}(T) \xrightarrow{\Gamma} \mathrm{AutG/T} \times \mathrm{AutT} \xrightarrow{\pi_{G/T}} \mathrm{AutG/T}$. Let $\mathrm{Ker}(\Gamma\, \pi|_{G/T}) = (\mathrm{AutG})^+$.

Then $\mathrm{InnG} \leq (\mathrm{AutG})^+ \leq \mathrm{AutG}$ and since AutG/T has order two the index of $(\mathrm{AutG})^+$ in AutG is at most two. We are interested in $(\mathrm{AutG})^+$ because it contains all nilpotent automorphisms of G . For we showed in chapter 1 that if γ is an automorphism of G then γ lies in NilG if and only if $\gamma\Gamma$ lies in $\mathrm{NilG/T} \times \mathrm{NilT}$. Now G/T is infinite cyclic so $\mathrm{NilG/T} = 1$ and so γ lies in NilG if and only if γ lies in $(\mathrm{AutG})^+$ and $\gamma\Delta$ lies in NilT .

Let B be a subgroup of AutT containing InnT and such that $B/\mathrm{InnT} = \overline{B} = \langle \overline{\alpha} \in \mathrm{OutT} \mid \overline{\phi}^{\overline{\alpha}} = \overline{\phi}$ or $\overline{\phi}^{\overline{\alpha}} = \overline{\phi}^{-1} \rangle$, the extended centraliser of $\overline{\phi}$ in OutT , and let $B^+ \leq B$ be such that

$B^+/\mathrm{InnT} = \overline{B}^+ = \langle \overline{\alpha} \in \mathrm{OutT} \mid \overline{\phi}^{\overline{\alpha}} = \overline{\phi} \rangle$, the centraliser of $\overline{\phi}$ in OutT .

Then $\overline{B}^+ = C_{\mathrm{OutT}}((G/T)\chi)$. Let

$X_1 = \{ \gamma : z \longrightarrow z^a c^{1+(-1)^a} s \; , \gamma|_T = 1_T \mid a \in \{1,-1\}, s \in Z(T) \}$.

Let $X_2 = \{ \gamma : z \longrightarrow z^a c^{\frac{1+(-1)^a}{2}} s \; , \gamma|_T = 1_T \mid a \in \{1,-1\}, s \in Z(T) \}$.

We can now describe the exact sequences determined by Δ in terms of these groups.

3.1.1 <u>Theorem</u> There exist exact sequences of groups as follows.

$$1 \longrightarrow V_\chi \longrightarrow \mathrm{Inn}G \xrightarrow{\Delta} \langle \phi, \mathrm{Inn}T \rangle \longrightarrow 1$$

$$1 \longrightarrow Z(T) \longrightarrow (\mathrm{Aut}G)^+ \xrightarrow{\Delta} B^+ \longrightarrow 1$$

$$1 \longrightarrow Z(T) \longrightarrow \mathrm{Aut}G \xrightarrow{\Delta} B \longrightarrow 1 \quad \text{if} \quad |(G/T)\chi| > 2$$

$$1 \longrightarrow X_i \longrightarrow \mathrm{Aut}G \xrightarrow{\Delta} B \longrightarrow 1 \quad \text{if} \quad |(G/T)\chi| = i \leqslant 2 .$$

<u>Proof</u> Suppose $\gamma \in \mathrm{Aut}G$ and that $\gamma \Gamma . \pi|_{G/T} = \gamma|_{G/T} : zT \longrightarrow z^{a_\gamma}T$ where $a_\gamma \in \{1,-1\}$. Then $\gamma : z \longrightarrow z^{a_\gamma}t_\gamma$ for some $t_\gamma \in T$, and γ determines $\gamma\Delta \in \mathrm{Aut}T$.

Now given any triple $a \in \{1,-1\}$, $t \in T$, $\eta \in \mathrm{Aut}T$, the map $\theta : z \longrightarrow z^a t$, $\theta : y \longrightarrow y\eta$ for all $y \in T$ is injective (as $(z^i y)\theta = 1$ if and only if $(z^a t)^i (y\eta) = 1$ if and only if $z^i \in T$ if and only if $i = 0$ and $y = 1$) and surjective as it is surjective on G/T and T.

θ defines an automorphism of G

$\Leftrightarrow$ $(z^i r)\theta(z^j s)\theta = (z^i r z^j s)\theta$ for all $i,j \in \mathbb{Z}$, $r,s \in T$

$\Leftrightarrow$ $(z^a t)^i . r\eta . (z^a t)^j . s\eta = (z^a t)^{i+j} . (r[r,z^j]s)\eta$

$\Leftrightarrow$ $[r\eta, (z^a t)^j] = [r, z^j]\eta$

$\Leftrightarrow$ $(r\eta)^{(z^a t)^j} = (r^{z^j})\eta$ for all $r \in T$, $j \in \mathbb{Z}$

$\Leftrightarrow$ $\eta(\phi^a \mu_t)^j = \phi^j \eta$ for all j

$\Leftrightarrow$ $\eta \phi^a \mu_t = \phi \eta$ (since $\eta(\phi^a \mu_t)^{j-1} = \phi^{j-1}\eta$ and $\eta\phi^a\mu_t = \phi\eta$ imply $\eta(\phi^a\mu_t)^j = \phi\eta . \eta^{-1}\phi^{j-1}\eta = \phi^j \eta$)

$\Leftrightarrow$ $\phi^a \mu_t = \phi^\eta$.

This calculation shows that if $\gamma \in \mathrm{Aut}T$ and $\gamma : z \longrightarrow z^{a_\gamma} t_\gamma$ then $\phi^{a_\gamma}\mu_{t_\gamma} = \phi^{\gamma\Delta}$, that is $\bar{\phi}^{a_\gamma} = \bar{\phi}^{\overline{\gamma\Delta}}$ and $\gamma\Delta \in B$. If $\gamma \in (\mathrm{Aut}G)^+$ then $a_\gamma = 1$ and $\gamma\Delta \in B^+$. Furthermore $\Delta : \mathrm{Aut}G \longrightarrow B$ and $\Delta : (\mathrm{Aut}G)^+ \longrightarrow B^+$ are surjective, since given $\zeta \in B$, $\zeta^+ \in B^+$ then $\phi^\zeta = \phi^a \mu_t$ for some $a \in \{1,-1\}$ and some $t \in T$ and $\phi^{\zeta^+} = \phi\mu_{t^+}$

for some $t^+ \in T$, so the above calculation shows that if λ and λ^+ are defined by $\lambda : z \longrightarrow z^a t$ $\lambda|_T = \mathfrak{Z}$ and $\lambda^+ : z \longrightarrow zt$ $\lambda^+|_T = \mathfrak{Z}^+$ then λ, λ^+ are elements of $\mathrm{Aut}G$, $(\mathrm{Aut}G)^+$ respectively satisfying $\Delta : \lambda \longrightarrow \mathfrak{Z}$ and $\Delta : \lambda^+ \longrightarrow \mathfrak{Z}^+$.

The sequences (2), (3) and (4) will all arise from consideration of $\mathrm{Ker}\,\Delta$, since $1 \longrightarrow \mathrm{Ker}\Delta \longrightarrow \mathrm{Aut}G \longrightarrow \mathrm{Im}\,\Delta = B \longrightarrow 1$ and $1 \longrightarrow \mathrm{Ker}\,\Delta \longrightarrow (\mathrm{Aut}G)^+ \longrightarrow \mathrm{Im}\Delta = B^+ \longrightarrow 1$ are exact.
Suppose $\gamma \in \mathrm{Aut}G$, where $z\gamma = z^{a_\gamma} t_\gamma$ for some $a_\gamma \in \{1\ -1\}$, and suppose that $\gamma^\Delta = 1_T$. Then $\phi^{a_\gamma}\mu_{t_\gamma} = \phi^{\gamma\Delta} = \phi$. If $a_\gamma = 1$, that is if $\gamma \in (\mathrm{Aut}G)^+$, then $\phi\mu_{t_\gamma} = \phi$ so $t_\gamma \in Z(T)$. Conversely given $u \in Z(T)$ the map $\delta : G \longrightarrow G$ defined by $\delta : z \longrightarrow zu$, $\delta : t \longrightarrow t$ for all $t \in T$ lies in $(\mathrm{Aut}G)^+$, and $\delta\Delta = 1_T$. Thus we have set up a bijection between $(\mathrm{Aut}G)^+ \cap \mathrm{Ker}\,\Delta$ and $Z(T)$, defined by $\gamma \longrightarrow z^{-1}.z\gamma$.

If $a_\gamma = -1$ then $\phi^{-1}\mu_{t_\gamma} = \phi$ and $\phi^2 = \mu_{t_\gamma}$, so this can only happen when $\phi^2 \in \mathrm{Inn}T$, that is when $m = |(G/T)\chi| \leq 2$.
If $m = 1$ then $\phi = \mu_c$ for some $c \in T$ and $\phi^2 = \mu_{c^2}$. $\mathrm{Ker}\Delta \cap (\mathrm{Aut}G)^+$ has index 2 in $\mathrm{Ker}\,\Delta$ and the quotient is generated by $\sigma.\mathrm{Ker}\,\Delta \cap (\mathrm{Aut}G)^+$ where $z\sigma = z^{-1}c^2$ and $t\sigma = t$ for all $t \in T$. Then it is easy to see that $\mathrm{Ker}\,\Delta$ is X_1, and we have verified (4) in case $i = 1$.
If $m = 2$ then $\phi^2 = \mu_c$ for some $c \in T$; $\mathrm{Ker}\Delta/(\mathrm{Ker}\,\Delta \cap (\mathrm{Aut}G)^+)$ has order two and is generated by $\eta\,.\,\mathrm{Ker}\,\Delta \cap (\mathrm{Aut}G)^+$ where $z\eta = z^{-1}c$ and $t\eta = t$ for all $t \in T$. We can check that $\mathrm{Ker}\Delta = X_2$, verifying (4) in case $i = 2$.

If m is at least three then a_γ is always equal to 1 and $\mathrm{Ker}\Delta \subseteq (\mathrm{Aut}G)^+$. Thus to complete our proof of sequences (2) and (3) we need to show that the bijection between $\mathrm{Ker}\Delta \cap (\mathrm{Aut}G)^+$ and $Z(T)$ established above is an isomorphism. To do this, given γ in $\mathrm{Ker}\Delta \cap (\mathrm{Aut}G)^+$ define $\gamma\Lambda = z^{-1}.z\gamma \in Z(T)$. Then if $\alpha, \beta \in \mathrm{Ker}\Delta \cap (\mathrm{Aut}G)^+$

$$(\alpha\beta)\Lambda = z^{-1}.(z\alpha\beta) = (z^{-1}.z\beta)(z^{-1}.z\alpha)\beta = (z^{-1}.z\beta)(z^{-1}.z\alpha) \quad \text{as} \quad \beta|_T = 1_T$$
$$= (z^{-1}.z\alpha)(z^{-1}.z\beta) \quad \text{as} \quad z^{-1}.z\alpha \in Z(T)$$
$$= (\alpha\Lambda)(\beta\Lambda)$$

and so Λ is an isomorphism.

Considering (1) we see that $V\alpha \leq Z(T)$, $\mathrm{Inn}G \leq (\mathrm{Aut}G)^+$ and $\langle\phi,\mathrm{Inn}T\rangle \leq B^+$, so it suffices to show that $\mathrm{Inn}G.\Delta = \langle\phi.\mathrm{Inn}T\rangle$ and $(\mathrm{Ker}\Delta|_{\mathrm{Inn}G})\Lambda = V\alpha$. Since the diagram

$$\begin{tikzcd} G \arrow[r, dashed] \arrow[dr, "\rho"'] & \mathrm{Inn}G \arrow[d, "\Delta"] \\ & \mathrm{Aut}T \end{tikzcd}$$

commutes, we see that $\mathrm{Inn}G.\Delta = G\rho = \langle\phi,\mathrm{Inn}T\rangle$. Given $f \in \mathrm{Ker}\Delta|_{\mathrm{Inn}G}$ we know that f is conjugation by some $z^i t$ in G . Then $f\Lambda = z^{-1}.zf = z^{-1}.z^{z^i t} = t^{-1}\phi.t$, and to show that $(\mathrm{Ker}\Delta|_{\mathrm{Inn}G})\Lambda \leq V\alpha$ it suffices to show that $t \in V$, which shows that $f\Lambda = t\alpha$. Now $f|_T = 1_T$ so $z^i t \in C_G(T)$ and $\phi^i = \mu_{t^{-1}} \in \mathrm{Inn}T \cap \langle\phi\rangle = \langle\mu_c\rangle$ so $t \in \langle c, Z(T)\rangle = V$. Finally we need to show that $V\alpha \leq (\mathrm{Ker}\Delta|_{\mathrm{Inn}G})\Lambda$. Given $s \in V\alpha$ then $s = u\alpha = z^{-1}u^{-1}zu$ for some $u \in V$. Suppose that $u = c^i x$ for some integer i and some x in $Z(T)$. Then if θ is conjugation by $z^{-mi}c^i x$ in G , θ centralises T , so lies in $\mathrm{Ker}\Delta|_{\mathrm{Inn}G}$ and $\theta\Lambda = z^{-1}.z\theta = z^{-1}z^u = s$ as required. Thus (1) is exact.

The next lemma tells us what happens to $\mathrm{Nil}G$ under the action of Δ .

3.1.2 <u>Lemma</u> If $\Delta : \mathrm{Aut}G \longrightarrow \mathrm{Aut}T$ then $\mathrm{Ker}\Delta \cap \mathrm{Nil}G = (\mathrm{Aut}G)^+ \cap \mathrm{Ker}\Delta$ and the image of $\mathrm{Nil}G$ under Δ is $B^+ \cap \mathrm{Nil}T$.

<u>Proof</u> If γ lies in $\mathrm{Aut}G$ then as we remarked above γ lies in $\mathrm{Nil}G$ if and only if γ lies in $(\mathrm{Aut}G)^+$ and $\gamma\Delta$ lies in $\mathrm{Nil}T$. $\gamma \in \mathrm{Nil}G \cap \mathrm{Ker}\Delta$ if and only if $\gamma|_T = 1_T$ and $\gamma \in (\mathrm{Aut}G)^+$

and $\gamma\Delta$ lies in NilT, if and only if γ lies in $(\mathrm{Aut}G)^{+} \cap \mathrm{Ker}\Delta$ since 1_T obviously lies in NilT. We have shown in (2) of the previous theorem that $(\mathrm{Aut}G)^{+}.\Delta = B^{+}$, so it follows that $(\mathrm{Nil}\zeta)\Delta = B^{+} \cap \mathrm{Nil}T$.

We use this lemma and the sequences of 3.1.1 to give us conditions under which G has no non-inner automorphisms acting nilpotently.

3.1.3 <u>Criterion</u> Let G be a finitely generated nilpotent group with Hirsch length one. Let T be its torsion subgroup and let ϕ be an automorphism of T induced by conjugation by a generator of G/T. Let $\langle \mu_c \rangle = \langle \phi \rangle \cap \mathrm{Inn}T$. Then NilG = InnG if and only if both

$B^{+} \cap \mathrm{Nil}T = \langle \phi, \mathrm{Inn}T \rangle$ (A) and

$Z(T) = [\phi, \langle c, Z(T) \rangle]$ (B) hold.

If further T is a p-group then condition (A) becomes $|C_{\mathrm{Out}T}(\bar{\phi}) : \langle \bar{\phi} \rangle|$ is not divisible by p.

<u>Proof</u> NilG contains InnG so they are equal if and only if $(\mathrm{Nil}G)\Delta = (\mathrm{Inn}G)\Delta$ and $\mathrm{Nil}G \cap \mathrm{Ker}\Delta = \mathrm{Inn}G \cap \mathrm{Ker}\Delta$. The first sequence of 3.1.1 shows that $(\mathrm{Inn}G)\Delta = \langle \phi, \mathrm{Inn}T \rangle$ so that applying 3.1.2 we see that $(\mathrm{Nil}G)\Delta = (\mathrm{Inn}G)\Delta$ if and only if $B^{+} \cap \mathrm{Nil}T = \langle \phi, \mathrm{Inn}T \rangle$. $\mathrm{Nil}G \cap \mathrm{Ker}\Delta = (\mathrm{Aut}G)^{+} \cap \mathrm{Ker}\Delta$ which is isomorphic to Z(T) under $\wedge$ as shown in (2) of 3.1.1. $\mathrm{Inn}G \cap \mathrm{Ker}\Delta$ is isomorphic under $\wedge$ to $V\alpha = [\phi, \langle c\ Z(T) \rangle]$ (sequence (1)) and (B) follows.

If T is a p-group then NilT is just the set of elements of AutT of p-power order, so $B^{+} \cap \mathrm{Nil}T = \langle \phi, \mathrm{Inn}T \rangle$ if and only if $\langle \phi, \mathrm{Inn}T \rangle$ consists of the elements of B^{+} of p-power order. $\langle \phi, \mathrm{Inn}T \rangle$ is normal in B, so this happens whenever $\langle \phi, \mathrm{Inn}T \rangle$ is the unique Sylow p-subgroup of B, that is whenever $\langle \bar{\phi} \rangle$ is the unique Sylow p-subgroup of $\overline{B}^+ = C_{OutT}(\overline{\phi})$, that is whenever $|C_{OutT}(\overline{\phi}):\langle\overline{\phi}\rangle|$ is not divisble by p .

It is this criterion which enables us to get a hold on the problem. The existence of non-inner automorphisms of certain groups follows from it fairly easily and will be discussed in the next section.

We conclude this section with examples to show that (A) and (B) can both occur and are independent. It suffices to construct finitely generated nilpotent groups of Hirsch length one satisfying respectively (A) but not (B) and (B) but not (A). Our remarks in the introduction to this chapter show that it suffices to exhibit a finite group T and $\phi \in$ AutT acting nilpotently on T such that the pair (T,ϕ) satisfy (A) but not (B) (or (B) but not (A)).

We shall show in section 4.3 that if T is the semidihedral group of order 2^m $(m \geq 4)$ then OutT is cyclic of order 2^{m-2}. Thus if ϕ is an element of AutT such that ϕ InnT generates OutT the pair (T,ϕ) satisfies (A). We shall show in 4.3.1 that (T,ϕ) fails to satisfy (B).

On the other hand the following family of groups satisfy (B) but not (A).

<u>Example</u> Let n be a positive integer and let p be a prime not equal to 2 or 3. Let $T_n = \langle a,b \mid a^{p^{n+1}} = b^{p^{n+1}} = 1, a^b = a^{1+p} \rangle$, and let $\phi : T_n \longrightarrow T_n$ be defined by $\phi : b \longrightarrow ba$ $\phi : a \longrightarrow ab^{p^n}$. I claim that ϕ is an automorphism of T_n and that the pair (T,ϕ) satisfy (B) but not (A).

We observe first that $Z(T_n) = \langle a^{p^n}, b^{p^n} \rangle$ and $T_n' = \langle a^p \rangle$. ϕ is a bijection and ϕ is an automorphism since

$(a\phi)^{p^n} = (ab^{p^n})^{p^n} = a^{p^n}$ (as $b^{p^n} \in Z(T_n)$) so $|a\phi| = |a|$.

$(b\phi)^{p^n} = (ba)^{p^n} = b^{p^n} a^{b^{p^n-1}} . a^{b^{p^n-2}} . \ldots\ldots . a = b^{p^n} . a^x$ where

$x = (1+p)^{p^n-1} + \ldots + (1+p) + 1$

$= \{(1+p)^{p^n} - 1\}/p$

$= p^n + p^{n+1}.y$ for some integer y

so $(b\phi)^{p^n} = b^{p^n} a^{p^n}$ and $|b\phi| = |b|$.

$(a^b)\phi = (ab^{p^n})^{ba} = a^b = a^{p+1} = (ab^{p^n})^{p+1} = (a\phi)^{p+1} = a^{p+1}\phi$, and so ϕ preserves the relations of T_n and must be an automorphism.

We now work out the action of powers of ϕ .

$a\phi = ab^{p^n}$ and $b^{p^n}\phi = b^{p^n}a^{p^n}$, $a^{p^n}\phi = a^{p^n}$ so

$a\phi^i = ab^{p^n x_i} a^{p^n y_i}$ for some integers x_i, y_i with $x_1 = 1$ and $y_1 = 0$ and $a\phi^{i+1} = ab^{p^n(x_i+1)} a^{p^n(y_i+x_i)}$. Solving for x_i and y_i shows that $x_i = i$ and $y_i = \frac{1}{2}i(i-1)$, so in particular $a\phi^p = a$ as $p \neq 2$.

$b\phi = ba$ and $a\phi = ab^{p^n}$ so $b\phi^i = ba^{u_i} b^{p^n v_i} a^{p^n w_i}$ some $u_i\ v_i\ w_i \in \mathbb{Z}$, and $b\phi^{i+1} = ba^{u_i+1} . b^{p^n(v_i+u_i)} . a^{p^n(w_i+v_i)}$. Solving these relations shows that $u_i = i$, $v_i = \frac{1}{2}i(i-1)$ and $w_i = i(i-1)(i-2)/6$ and so $b\phi^p = ba^p$ as p is not 2 or 3. It follows that $\phi^p = \mu_{a^{-1}}$ as $b^{a^{-1}} = aba^{-1} = b.b^{-1}aba^{-1} = ba^p$.

ϕ is not inner so we may assume that $\langle\phi\rangle \cap \mathrm{Inn}T = \mu_a$, so that $V = \langle a, Z(T)\rangle$. It remains to show that $V\alpha = Z(T)$.

$V\alpha = \langle a^{-1}, a^{p^n}, b^{p^n}\rangle\alpha = \langle a\phi.a^{-1}, b^{-p^n}\phi.b^{p^n}\rangle = \langle ab^{p^n}a^{-1}, b^{-p^n}a^{-p^n}b^{p^n}\rangle$

$= \langle b^{p^n}, a^{-p^n}\rangle = Z(T)$ as required so (T,ϕ) satisfies (B).

To show that (T,ϕ) does not satisfy (A) we construct an automorphism ψ of T which lies in $\mathrm{Nil}T \cap B^+$ but not in $\langle\phi, \mathrm{Inn}T\rangle$. Let $\psi : b \longrightarrow b^{1+p^n}$, $\psi : a \longrightarrow a$. Then $\psi \in \mathrm{Aut}T$ and ψ is not inner as $b^{-1}\psi.b$ does not lie in T' . Any non inner element of $\langle\phi, \mathrm{Inn}T\rangle$ has the form $\phi^i\mu_d$ where $1 \leq i \leq p-1$ and $d \in T$, so $\phi^i\mu_d$ does not centralise a , so $\psi \notin \langle\phi, \mathrm{Inn}T\rangle$. Now

$a\phi\psi\phi^{-1}\psi^{-1} = a$ and $b\phi\psi\phi^{-1}\psi^{-1} = (bab^{p^n})\phi^{-1}\psi^{-1} = (b^{1+p^n}a^{-p^n})\psi^{-1} = ba^{-p^n}$

so $[\phi^{-1}, \psi^{-1}]$ acts on T as conjugation by $a^{p^{n-1}}$ and $\psi \in B^+$. ψ has p-power order so ψ lies in NilT. Thus $\mathrm{NilT} \cap B^+$ is strictly larger than $\langle \phi, \mathrm{InnT} \rangle$ so (A) is not satisfied .

Section 3.2

The descriptions of AutG and $(\mathrm{AutG})^+$ which we obtained in the previous section, and the criterion which followed from them, are used here to show that certain classes of finitely generated nilpotent groups admit non-inner automorphisms: in particular those of nilpotency class two and order at least three .

First of all we look at those groups where $\mathrm{Ker}\Delta \nleq (\mathrm{AutG})^+$, that is the groups with $|(G/T)\chi| \leq 2$.

3.2.1 Theorem Let G be a finitely generated nilpotent group with Hirsch length one and torsion subgroup T . Let $\chi : G/T \longrightarrow \mathrm{OutT}$ be the coupling associated with G . Suppose $|(G/T)\chi| \leq 2$. Then G has a non-inner automorphism inducing inversion on G/T and so not acting nilpotently.

Proof We have from 3.1.1 that $1 \longrightarrow X_m \longrightarrow \mathrm{AutG} \longrightarrow B \longrightarrow 1$ is exact for m equal to 1 or 2, where $X_m = \mathrm{Ker}\Delta$. It follows from the proof of 3.1.1 that $|X_m : X_m \cap (\mathrm{AutG})^+| = 2$. Now $\mathrm{InnG} \leq (\mathrm{AutG})^+$, so any element of $X_m \backslash (\mathrm{AutG})^+$ is a non-inner automorphism of G , and induces inversion on G/T ; as it does not act nilpotently on G/T it does not act nilpotently on G .

Turning our attention to non-inner automorphisms acting nilpotently, we concentrate in this section on automorphisms which arise because part (B) of the criterion fails to hold. When this happens G has a non-inner automorphism θ of the form $\theta : z \longrightarrow zt$ for some $t \in Z(T)$, and $\theta|_T = 1$. Then $\theta^i : z \longrightarrow zt^i$ so the order of θ is just the order of t ; in particular $|\theta| \,\big|\, |Z(T)|$.

θ centralises the series $1 \lhd T \lhd G$ so θ acts nilpotently on G .

3.2.2 **Theorem** If G is a finitely generated nilpotent group with Hirsch length one and non-trivial torsion subgroup T and one of the following holds then $C_{\mathrm{Aut}G}(G/T,T)$ contains a non-inner automorphism of G acting nilpotently on G and of order dividing $|Z(T)|$.

(a) T is abelian.

(b) $(G/T)\chi = 1$ where $\chi : G/T \longrightarrow \mathrm{Out}T$ is the coupling associated with G .

(c) $G\rho$ splits over $\mathrm{Inn}T$.

Proof We note first that if U is a normal subgroup of G then $[G,U] \lneqq U$ as G is nilpotent. Thus if $U \leq V = \langle c,Z(T)\rangle$ and $U\phi = U$, $U\alpha = [\phi,U] \leq [G,U] \lneqq U$.

If T is abelian $\mathrm{Inn}T = 1$, so $G\rho$ splits over $\mathrm{Inn}T$ and (a) is a special case of (c). If $(G/T)\chi = 1$ then the definition of χ by the commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\rho} & \mathrm{Aut}T \\ \downarrow & & \downarrow \\ G/T & \xrightarrow{\chi} & \mathrm{Out}T \end{array}$$

shows that $G\rho \leq \mathrm{Inn}T$, so $G\rho$ splits over $\mathrm{Inn}T$ and (b) is a special case of (c).

To prove (c) we notice that if $G\rho$ splits over $\mathrm{Inn}T$ then we can choose $\phi \in G\rho$ such that $G\rho = \mathrm{Inn}T \rtimes \langle\phi\rangle$, so in particular $\langle\phi\rangle \cap \mathrm{Inn}T = 1$. $\phi = z\rho$ where zT is some generator of G/T , and so we may apply our previous theory with this choice of ϕ . Since $\langle\phi\rangle \cap \mathrm{Inn}T = 1$, $c \in Z(T)$ so $V = \langle c,Z(T)\rangle = Z(T)$ and $V\alpha \lneqq V = Z(T)$ by the remark at the beginning of the theorem. Thus (B) of the criterion does not hold, and so as we remarked above, G has an outer automorphism of the required form.

We come now to the main result of this section.

3.2.3 **Theorem** Let G be a finitely generated nilpotent group of nilpotency class 2 with Hirsch length one. Let T be the torsion subgroup of G. Then $C_{\mathrm{Aut}G}(G/T, T)$ contains a non-inner automorphism of T acting nilpotently on T of order dividing $Z(T)$.

Proof Select a $z \in G$ such that zT is generator of G/T, and let $\phi = z\rho \in \mathrm{Aut}T$. If (B) does not hold then the remarks before 3.2.2 show that G has a non-inner automorphism of the required form. So we may assume that (B) holds, that is $Z(T) = V\alpha = \{v^{-1}\phi.v \mid v \in V\} = \{[z,v] \mid v \in V\}$, so $Z(T) \leqslant G'$. Now G/T is cyclic, so $G' \leqslant T$. G has class 2, so $G' \leqslant Z(G)$, so $G' \leqslant Z(G) \cap T \leqslant Z(T)$. Thus we have $G' = Z(G) \cap T = Z(T)$.

If $u \in Z(T)$ then $u \in Z(G)$ so $u\alpha = u^{-1}\phi.u = [z,u] = 1$, and $Z(T) \leqslant \mathrm{Ker}\,\alpha$, so $V/\mathrm{Ker}\alpha$ is a quotient of $V/Z(T)$ and $|V:\mathrm{Ker}\alpha| \leqslant |V:Z(T)|$. $V/Z(T) = \langle c.Z(T)\rangle$ where $\mu_c = \phi^m$, and the order of μ_c is just the order of $cZ(T)$ in $T/Z(T)$ so $|\phi^m| = |\mu_c| = |V:Z(T)| \geqslant |V:\mathrm{Ker}\,\alpha|$. $|V:\mathrm{Ker}\,\alpha| = |V\alpha| = |Z(T)|$ (using the first isomorphism theorem) so $|\phi^m| \geqslant |Z(T)|$.

Now consider the action of ϕ on T. Given $t \in T$, $t\phi = t[t,z]$ where $[t,z] \in G' = Z(T) = Z(G) \cap T$. So $[t,z]\phi = [t,z]^z = [t,z]$, and $t\phi^i = t[t,z]^i$ for all $i \in \mathbb{Z}$. Thus $|\phi| \leqslant \exp(G') \leqslant |G'| = |Z(T)| \leqslant |\phi^m|$. Since ϕ is a generator of $\langle\phi\rangle$, this shows that $\phi^m = \mu_c$ is also a generator of $\langle\phi\rangle$ and so $\langle\phi\rangle \leqslant \mathrm{Inn}T$, that is $m = |(G/T)\chi| = 1$, and so by 3.2.2 G has an outer automorphism of the required form.

We come now to the main result of this section.

3.2.3 **Theorem** Let G be a finitely generated nilpotent group of nilpotency class 2 with Hirsch length one. Let T be the torsion subgroup of G. Then $C_{\mathrm{Aut}G}(G/T,T)$ contains a non-inner automorphism of T acting nilpotently on T of order dividing $Z(T)$.

<u>Proof</u> Select $z \in G$ such that zT is a generator of G/T, and let $\phi = z\rho \in \mathrm{Aut}T$. If (B) does not hold then the remarks before 3.2.2 show that G has a non-inner automorphism of the required form. So we may assume that (B) holds, that is $Z(T) = V\alpha = \{v^{-1}\phi.v \mid v \in V\} = \{[z,v] \mid v \in V\}$, so $Z(T) \leqslant G'$. Now G/T is cyclic, so $G' \leqslant T$. G has class 2, so $G' \leqslant Z(G)$, so $G' \leqslant Z(G) \cap T \leqslant Z(T)$. Thus we have $G' = Z(G) \cap T = Z(T)$.

If $u \in Z(T)$ then $u \in Z(G)$ so $u\alpha = u^{-1}\phi.u = [z,u] = 1$, and $Z(T) \leqslant \mathrm{Ker}\,\alpha$, so $V/\mathrm{Ker}\,\alpha$ is a quotient of $V/Z(T)$ and $|V{:}\mathrm{Ker}\,\alpha| \leqslant |V{:}Z(T)|$. $V/Z(T) = \langle c.Z(T)\rangle$ where $\mu_c = \phi^m$, and the order of μ_c is just the order of $cZ(T)$ in $T/Z(T)$ so $|\phi^m| = |\mu_c| = |V{:}Z(T)| \geqslant |V{:}\mathrm{Ker}\,\alpha|$. $|V{:}\mathrm{Ker}\,\alpha| = |V\alpha| = |Z(T)|$ (using the first isomorphism theorem) so $|\phi^m| \geqslant |Z(T)|$.

Now consider the action of ϕ on T. Given $t \in T$, $t\phi = t[t,z]$ where $[t,z] \in G' = Z(T) = Z(G) \cap T$. So $[t,z]\phi = [t,z]^z = [t,z]$, and $t\phi^i = t[t,z]^i$ for all $i \in \mathbb{Z}$. Thus $|\phi| \leqslant \exp(G') \leqslant |G'| = |Z(T)| \leqslant |\phi^m|$. Since ϕ is a generator of $\langle\phi\rangle$, this shows that $\phi^m = \mu_c$ is also a generator of $\langle\phi\rangle$ and so $\langle\phi\rangle \leqslant \mathrm{Inn}T$, that is $m = |(G/T)\chi| = 1$, and so by 3.2.2 G has an outer automorphism of the required form.

3.2.4 **Corollary** Any finitely generated nilpotent group of nilpotency class 2 with at least three elements admits a non-inner automorphism.

Proof If G is finite the result follows from Gaschütz' theorem 2.3.2, if G has Hirsch length one from the previous theorem and if G has Hirsch length at least two from the result of Baumslag which we proved in chapter 1.

We remark that the hypothesis that G be finitely generated is necessary because of examples due to Heineken and Zaleskii.

Section 3.3

As we remarked in chapter 1, in looking for non-inner automorphisms of a finitely generated nilpotent group G with Hirsch length one it is enough to consider the case when T, the torsion subgroup of G, and $(G/T)\chi$, where $\chi : G/T \longrightarrow \mathrm{Out}T$ is the coupling associated to G, are both p-groups. We prove this assertion in this section and define the concept of an admissible pair (T,ϕ) where T is a finite p-group and ϕ is an automorphism of T of p-power order. In what follows certain abelian sections of T will be regarded as $K\langle\phi\rangle$ modules where K is the field of p elements, so we shall recall some properties of such modules before investigating some consequences of the definition of an admissible pair.

3.3.1 Lemma Suppose G is a finitely generated nilpotent group with Hirsch length one, and let $G = \langle z,T\rangle$ where T is the torsion subgroup of G. Let $\chi : G/T \longrightarrow \mathrm{Out}T$ be the coupling associated with G. Suppose $T = P \times Q$ where P is a non-trivial p-group and Q is a group of order prime to p. Then

1) Let $H = \langle z,P\rangle$ and suppose that $\mathrm{Nil}H$ does not lie in $\mathrm{Inn}H$. Then $\mathrm{Nil}G$ does not lie in $\mathrm{Inn}G$.

2) Suppose that $P = T$. Then $(G/T)\chi$ is a p-group.

Proof 1) Q is characteristic in T, which is normal in G, so Q is normal in G. Similarly P is normal in G, and so any element of H can be written in the form $z^i r$ for some integer i and some r in P, and any element of G can be expressed as qh for some $q \in Q$ and $h \in H$. Let θ be an element of $\mathrm{Nil}H$

which does not lie in InnH . Then θ lies in $(\mathrm{AutH})^+$. Define ψ on G by $\psi|_H = \theta$, $\psi|_Q = 1_Q$. $H \cap Q = 1$ so ψ is well-defined and bijective, and will be an automorphism if $[s, z^j\theta] = [s, z^j]$ for any integer j and any s in Q . But as $\theta \in (\mathrm{AutH})^+$, $z^j\theta = z^jr$ for some $r \in P$ so

$[s, z^j\theta] = [s, z^jr] = [s, r][s, z^j]^r = [s, z^j]$, as s and $[s, z^j]$ lie in Q , $r \in P$, and $[P, Q] = 1$. Thus ψ is an automorphism of G , and ψ acts nilpotently on G as ψ acts nilpotently on Q and H . ψ is not inner, as if ψ were conjugation by some qh with q in Q , and h in H we would have $g^{qh} = g\psi$ for all g in H , that is $g^{-1}g^q = g^{-1}(g\psi)^{h^{-1}}$. Q is normal in G so $g^{-1}g^q$ is an element of Q , and g lies in H , so $g^{-1}(g\psi)^{h^{-1}}$ lies in H , and thus if ψ were inner $g^{-1}g^q$ would lie in $H \cap Q$ which is trivial, and q would centralise H . But then ψ would act on H as conjugation by h , and ψ would be inner on H , contradicting our choice of θ . So ψ lies in NilG but not in InnG , as required.

2) Let $(G/T)\chi = \langle \bar{\phi} \rangle$ where ϕ is some automorphism of T . Since G is nilpotent ϕ acts nilpotently on T If $(G/T)\chi$ is not a p-group then some power of ϕ is a non-inner, and so non-trivial, automorphism of T of order prime to p acting nilpotently on the p-group T , which is impossible. Thus $(G/T)\chi$ is a p-group.

This lemma, together with the results in section 1, enable us to reduce the problem to a question about finite p-groups. We make the following definition.

<u>Definition</u> Let p be a prime. An admissible pair (T,ϕ) consists of a finite non-abelian p-group T and an automorphism ϕ of T of p-power order such that

$|C_{\mathrm{Out}T}(\bar{\phi}):\langle\bar{\phi}\rangle|$ is coprime to p (A)

$[\phi,\langle c,Z(T)\rangle] = Z(T)$ (B)

where $\langle\phi\rangle \cap \mathrm{Inn}T = \mu_c$.

3.3.2 <u>Theorem</u> There exists a finitely generated non-cyclic nilpotent group G with Hirsch length one and $\mathrm{Inn}G = \mathrm{Nil}G$ if and only if there exists an admissible pair for some prime p .

<u>Proof</u> If (T,ϕ) is admissible then the group $G = \langle z, T \mid t^z = t\phi \ \forall\, t \in T\rangle$ satisfies the conditions of 3.1.3 and so has $\mathrm{Inn}G = \mathrm{Nil}G$. Conversely given a finitely generated nilpotent group G with $\mathrm{Inn}G = \mathrm{Nil}G$ let T be its torsion subgroup and let p be a prime divisor of $|T| \neq 1$. Since T is a finite nilpotent group T can be expressed as $P \times Q$ where P is a p-group and Q is a group of order prime to p . Let $H = \langle z,P\rangle$ where z is a generator of G/T . Then the previous lemma shows that $\mathrm{Inn}H = \mathrm{Nil}H$. P is a p-group and since $\mathrm{Inn}H = \mathrm{Nil}H$ 3.2.2(a) shows that P is not abelian. Applying the second part of the previous lemma to H we deduce that the map $\psi : P \longrightarrow P$ defined by $q^z = q\psi$ for all q in P is an automorphism of P of p-power order. Since $\mathrm{Inn}H = \mathrm{Nil}H$, H satisfies (A) and (B) of 3.1.3 so the pair (P,ψ) is admissible.

We are going to obtain some properties of an admissible pair (T,ϕ) in terms of $K\langle\phi\rangle$ modules, where K is the field of p elements, so we list some well-known properties of such modules.

Let $A = \langle a \rangle$ be cyclic of order p^s for some $s \geqslant 1$, and let D be a finitely generated KA module. Then $C_D(A) \cong D/[D,A] \cong (C_p)^d$ where d is the number of direct summands in any decomposition of D into a direct sum of indecomposable KA modules. D is indecomposable if and only if $d = 1$, and in fact the following are equivalent.

(a) D is an indecomposable KA module

(b) $d = 1$

(c) $C_D(A)$ has order p.

(d) D is a uniserial KA module.

(e) D is a cyclic KA module.

We define the a-height of D to be $\min\{k \mid D(1-a)^k = 0\}$; then $k \leqslant p^s$ and k is the maximum of the a-heights of the indecomposable direct summands of D. An indecomposable KA module is free if and only if it is isomorphic to the regular KA module, that is if and only if it has a-height p^s, and so D has a free direct summand if and only if it has a-height equal to p^s. D will be a free KA module whenever $H^1(A,D) = 1$, that is whenever $C_D(A) = D\mathcal{J}$ where $\mathcal{J} : D \longrightarrow D$ is the trace map associated with a defined by $d\mathcal{J} = d(1+a+a^2 \ \ldots\ldots + a^{p^s-1})$ for all $d \in D$.

If D^* denotes the vector space dual of D then the following diagram defines a KA module structure on D^*, where $f : D \longrightarrow K$ is a typical element of D^*.

$$\begin{tikzcd} D \arrow[r, "a"] \arrow[d, "f"'] & D \arrow[d, "fa"] \\ K \arrow[r, "1"'] & K \end{tikzcd}$$

The lattice of KA submodules of D^* is just the inverse of that of D, so in particular D and D^* have the same a-height.

Our task in the rest of this section is to examine some properties of admissible pairs. We begin with some consequences of part (B) of the definition.

3.3.3 Theorem Let (T,ϕ) be admissible. Then $Z(T)/\mho_1(Z(T))$ is an indecomposable $K\langle\phi\rangle$ module generated by $c^{-1}.c\phi\mho_1(Z(T))$.

Proof Let $\mho_1(Z(T)) = W$. W and $Z(T)$ are characteristic in T so ϕ acts on $Z(T)/W$ which is an elementary abelian p-group and has the structure of a $K\langle\phi\rangle$ module. Since (T,ϕ) is admissible part (B) of the definition shows that $Z(T) = [\phi,\langle c,Z(T)\rangle]$ that is that $Z(T) = V\alpha$ where $V = \langle c,Z(T)\rangle$ and $\alpha : V \longrightarrow V$ is a ϕ-homomorphism defined by $v\alpha = v^{-1}\phi.v$ for all $v \in V$. Composing α with the quotient map $q : Z(T) \longrightarrow Z(T)/W$ yields a surjective ϕ-map $\alpha q : V \longrightarrow Z(T)/W$ such that $\mathrm{Ker}\alpha q = \{v \in V \mid v\alpha \in W\}$ $= \{v \in V \mid v\alpha \in \mho_1(V\alpha) = (\mho_1 V)\alpha\} = \{v \in V \mid v \in \mathrm{Ker}\alpha.\mho_1 V\}$.
Thus $Z(T)/W \underset{K\langle\phi\rangle}{\cong} V/\mathrm{Ker}\alpha.\mho_1 V$, and since quotients of indecomposable K modules are indecomposable it suffices to show that $V/\mho_1 V$ is indecomposable. Let $\underline{\ }$ denote images modulo $\mho_1 V$. Then $\underline{V}/[\phi,\underline{V}] = \underline{V}/\underline{V\alpha} \cong V/V\alpha.\mho_1 V = V/Z(T).\mho_1 V$, which is a quotient of the cyclic group $V/Z(T)$ and so is cyclic. $\underline{V}/[\phi,\underline{V}]$ has exponent p so it must have order p and it follows from our remarks above that $\underline{V}$ is indecomposable. Now $V/Z(T).\mho_1 V$ is generated by $c.Z(T).\mho_1 V$, so following the isomorphisms we see that $Z(T)/W$ is generated as a $K\langle\phi\rangle$ module by $c^{-1}.c\phi\mho_1(Z(T))$.

3.3.4 Corollary If (T,ϕ) is admissible then $Z(T)$ is generated as a $\mathbb{Z}\langle\phi\rangle$ module by $c^{-1}.c\phi$.

Proof $\mho_1 Z(T)$ is the Frattini subgroup of $Z(T)$ so since $Z(T)/\mho_1(Z(T))$ is generated as an abelian group by $\{(c^{-1}.c\phi)\phi^i\mho_1(Z(T)) \mid i \in \mathbb{Z}\}$ $Z(T)$ is generated as an abelian group by $\{(c^{-1}.c\phi)\phi^i \mid i \in \mathbb{Z}\}$ and as a $\mathbb{Z}\langle\phi\rangle$ module by $c^{-1}.c\phi$.

Turning to the consequences of part (A) of the definition we observe first the following result

3.3.5 Lemma Let (T,ϕ) be admissible. Then $\langle\bar{\phi}\rangle$ is a non-trivial subgroup of OutT.

Proof If $\bar{\phi}$ is trivial then, if $G = \langle z,T \mid t^z = t\phi \,\forall\, t \in T\rangle$, $(G/T)\chi = 1$, where χ is the coupling associated with G. But then $G\rho$ splits over InnT and 3.2.2(c) shows that NilG is not equal to InnG, so (T,ϕ) could not be admissible.

If (T,ϕ) is admissible we shall denote $|\bar{\phi}|$ by p^s.

Although it is possible to carry out a detailed analysis of finite groups G with a cyclic subgroup H of p-power order such that $C_G(H)/H$ has order coprime to p this does not seem to help in identifying groups whose automorphism groups have this property, and so we confine our analysis of the consequences of part (A) of the definition to those properties of OutT which appear to give useful information about T.

3.3.6 Lemma Let H be a finite group containing an element g of order $p^s \geqslant p$ such that $|C_H(g):\langle g\rangle|$ is coprime to p. Then if F is any p-subgroup of H which is normalised by g, $1 \lneq C_F(g) \leqslant \langle g\rangle$ and $g^{p^{s-1}} \in \Omega_1(Z(F))$.

If further F is elementary abelian then F is an indecomposable $K\langle g\rangle$ module.

__Proof__ $C_H(g)$ has a normal Sylow p-subgroup $\langle g\rangle$, which must contain all p-elements of $C_H(g)$. F is a p-group acted on by an element g of p-power order so $C_F(g) \neq 1$; $C_F(g)$ lies in $\langle g\rangle$ as it consists of p-elements of H which centralise $\langle g\rangle$. $\Omega_1(Z(F))$ is characteristic in F so it is normalised by g and by the same argument $1 \neq C_{\Omega_1(Z(F))}(g) \leq \langle g\rangle$. $\Omega_1(Z(F))$ has exponent p so $C_{\Omega_1(Z(F))}(g) = \langle g^{p^{s-1}}\rangle$. If F is elementary abelian then $F = \Omega_1(Z(F))$ and $C_F(g) = \langle g^{p^{s-1}}\rangle$ so has order p and F is an indecomposable $K\langle g\rangle$ module.

Applying this lemma to $\bar{\phi}$ in $\mathrm{Out}T$ yields

3.3.7 __Theorem__ Let (T,ϕ) be admissible. Then if F is a $\bar{\phi}$-invariant p-subgroup of $\mathrm{Out}T$ $1 \neq C_F(\bar{\phi}) \leq \langle\bar{\phi}\rangle$ and $\bar{\phi}^{p^{s-1}} \in \Omega_1(Z(F))$. If F is elementary abelian then F is $K\langle\bar{\phi}\rangle$ indecomposable.

__Proof__ Part (A) of the definition shows that $|C_{\mathrm{Out}T}(\bar{\phi}):\langle\bar{\phi}\rangle|$ is coprime to p and we can apply the previous lemma.

One application of this is the following

3.3.8 __Corollary__ Suppose that (T,ϕ) is admissible. Then if N is any normal and ϕ-invariant subgroup of T with $C_T(N) = Z(N)$ then either

$H^1(T/N, Z(N)) = 1$ or

$\bar{\phi}^{p^{s-1}} \in \overline{C_{\mathrm{Aut}T}(T/N,N)}$.

<u>Proof</u> Suppose $H^1(T/N,Z(N))$ is non-trivial. Then 2.1.2 shows that $C_{AutT}(T/N,N)$ does not lie in InnT, so $\overline{C_{AutT}(T/N,N)}$ is a non-trivial subgroup of OutT. Furthermore it is a p-group as T is, and ϕ-invariant as N is. Thus we can apply the previous result with $F = \overline{C_{AutT}(T/N,N)}$.

It would be nice to be able to develop this result by eliminating the second case and proving some lifting theorem akin to Schmid's (2.3.1) in the first. However since the result only gives information modulo InnT this programme seems rather difficult. Instead we work with subgroups of AutT rather than of OutT in what follows, basing our ideas on the following theorem.

3.3.9 <u>Theorem</u> Let (T,ϕ) be admissible and let H be an elementary abelian p-subgroup of AutT. Suppose that H is normalised by ϕ and that H is not contained in InnT . Then

1) There exists A , a $K\langle\phi\rangle$ indecomposable direct summand of H , and $\beta \in A\backslash(A \cap \mathrm{InnT})$ such that $H = A.H \cap \mathrm{InnT}$, $\overline{\beta} = \overline{\phi}^{p^{s-1}}$ and $[\phi,\beta] \in A \cap \mathrm{InnT}$.

2) If $[\phi,\beta] = \mu_y \in A \cap \mathrm{InnT}$ then Z(T) is generated as a $\mathbb{Z}\langle\phi\rangle$ module by $v.v\beta. \ \ldots \ .v\beta^{p-1}$ where $v \equiv y$ modulo Z(T).

<u>Proof</u> Let $H = \prod_{i=1}^{n} H_i$ be a decomposition of H as a direct product of indecomposable $K\langle\phi\rangle$ modules. Let $L = H \cap \mathrm{InnT}$. Then H/L is $K\langle\phi\rangle$ isomorphic to $\overline{H} = H.\mathrm{InnT}/\mathrm{InnT}$. $\overline{H}$ is a non-trivial elementary abelian p-subgroup of OutT , so 3.3.7 shows that $\overline{\phi}^{p^{s-1}} \in \overline{H}$ and $\overline{H}$ and hence H/L are indecomposable

$K\langle\phi\rangle$ modules. This means that H/L is uniserial so that if we choose H_iL to be maximal in $\{H_jL \mid 1 \leq j \leq n\}$, then $H_iL \geq H_jL$ for all $1 \leq j \leq n$ so $H \geq H_iL \geq \prod_{j=1}^{n} H_j = H$ and $H = H_iL = H_i.H \cap \mathrm{InnT}$. Let $H_i = A$.

Now $\overline{\phi}^{p^{s-1}} \in \overline{H}$ so let βL be the image of $\overline{\phi}^{p^{s-1}}$ in $H/L = A.L/L$. Then $\overline{\beta} = \overline{\phi}^{p^{s-1}}$, and β can be chosen to lie in A; thus $[\phi,\beta] \in A$ as A is a $K\langle\phi\rangle$ module. $\overline{[\phi,\beta]} = [\overline{\phi},\overline{\phi}^{p^{s-1}}] = 1$, and so $[\phi,\beta] \in A \cap \mathrm{InnT}$. β does not lie in $A \cap \mathrm{InnT}$ as $\phi^{p^{s-1}}$ does not lie in InnT.

2) Let $\beta\mu_t = \phi^{p^{s-1}}$ for some $t \in T$. We have
$\mu_y = [\phi,\beta] = [\phi, \phi^{p^{s-1}}\mu_{t^{-1}}] = [\phi, \mu_{t^{-1}}] = \mu_{t\phi.t^{-1}} = \mu_v$ where $v = t\phi.t^{-1}$.
Let $u_i = v.v\beta. \;\ldots\; .v\beta^{i-1}$ for $1 \leq i \leq p$, then $u_i^{-1}.u_{i-1} = v\beta^{i-1}$.
I claim $[\phi,\beta^i] = \mu_{u_i}$; this follows by using induction on i and the equation $[\phi,\beta^i] = [\phi,\beta][\phi,\beta^{i-1}]^{\beta}$. Let $x = t\beta^{p-1}. \;\ldots\; .t\beta.t$.
Then $\phi^{p^s} = (\beta\mu_t)^p = \beta^p\mu_x = \mu_x$, as H has exponent p, so we may set $c = x$ where $\langle\phi\rangle \cap \mathrm{InnT} = \langle\mu_c\rangle$.

$$
\begin{aligned}
\text{Then } c\phi &= t\beta^{p-1}\phi. \;\ldots\; .t\beta^{i}\phi. \;\ldots\; .t\phi \\
&= t\phi\beta^{p-1}[\beta^{p-1},\phi]. \;\ldots\; .t\phi\beta^{i}[\beta^{i},\phi]. \;\ldots\; .t\phi \\
&= (vt)\beta^{p-1}\mu_{u_{p-1}^{-1}}. \;\ldots\; .(vt)\beta^{i}\mu_{u_i^{-1}}. \;\ldots\; .(vt) \\
&= u_{p-1}.v\beta^{p-1}.c \\
&= u_p c,
\end{aligned}
$$

so $c^{-1}.c\phi = u_p$ and 3 3.4 shows that $Z(T)$ is generated as a module by $u_p = v.v\beta. \;\ldots\; .v\beta^{p-1}$. $\mu_y = \mu_v$ so $v \equiv y$ modulo $Z(T)$.

Chapter Four Subgroups of the automorphism group of a p-group

The main aim of this chapter is to examine certain abelian subgroups of the automorphism group of a finite p-group and to use them to obtain information about admissible pairs. Although we concentrate in 4.1 and 4.2 on two particular subgroups this idea could be applied to other subgroups and might give useful results. In 4.3 we digress to examine the automorphism groups of exceptional two groups.

The following elementary lemma explains how the automorphisms studied in this chapter arise.

4.0.1 **Lemma** Let G be a finite p-group and let A be a subgroup containing the Frattini subgroup of G. Let B be an elementary abelian subgroup of $Z(A)$. Then if $C = \{ \alpha \in \mathrm{Aut}G \mid \alpha|_A = 1 \text{ , } g^{-1}.g\alpha \in B \ \forall\ g \in G \}$, then $C \cong \mathrm{Der}_K(G/A,B)$ where K is the field of p elements, so in particular C is an elementary abelian p-group. If further ψ is an automorphism of G which normalises A and B then this is a ψ-isomorphism.

Proof Let bars denote images modulo A. If θ maps G/A to B then θ lies in $\mathrm{Der}_K(G/A,B)$ if and only if $(\bar{g}.\bar{h})\theta = (\bar{g}\theta)^h(\bar{h}\theta)$ for all $\bar{g}$, $\bar{h}$ in G/A. If ψ lies in $\mathrm{Aut}G$ and normalises A and B then $\mathrm{Der}_K(G/A,B)$ has a $K\langle\psi\rangle$ module structure given by the following diagram

$$\begin{array}{ccc} G/A & \xrightarrow{\psi} & G/A \\ \theta\downarrow & & \downarrow\theta^{\psi} \\ B & \xrightarrow[\psi]{} & B \end{array}$$

where θ is an element of $\mathrm{Der}_K(G/A,B)$.

We set up the isomorphism as follows. If $\alpha \in C$ define $\alpha\Gamma : G/A \longrightarrow B$ by $\alpha\Gamma : \bar{g} \longrightarrow g^{-1}.g\alpha$. It is routine to check that $\alpha\Gamma$ lies in $\mathrm{Der}_K(G/A,B)$ and that Γ is a homomorphism and a τ-map. We may also verify that if $\theta \in \mathrm{Der}_K(G/A,B)$ then the map $g \longrightarrow g.(\bar{g}\theta)$ for all $g \in G$ is an element of C, showing that Γ is an isomorphism.

Section 4.1

Let S be a non-abelian p-group and let ψ be an automorphism of S of p-power order. We are going to consider some properties of a certain maximal subgroup M of S with the aim of showing that if (S,ψ) is admissible then a particular subgroup of $C_{\mathrm{Aut}S}(S/M,M)$ lies in InnS.

S contains a maximal subgroup M with the property that M is normalised by ψ and M contains $Z(S)$. For since S is not abelian $S/Z(S)$ is a non-trivial p-group acted on by ψ, an automorphism of p-power order, so $S/Z(S)$ contains a maximal proper subgroup $M/Z(S)$ which is normalised by ψ. Then M has the required properties, and since $M \geqslant Z(S)$ we have $C_S(M) = Z(M)$. We shall denote $\Omega_1(Z(M)) = \{a \in Z(M) | a^p = 1\}$ by F. Of course F is normalised by ψ. We shall consider

$A_M = \{ \alpha \in \mathrm{Aut}S | M\alpha = M, \alpha|_M = 1_M, t^{-1}.t\alpha \in F \ \forall \ t \in S \}$.

Then 4.0.1 shows that A_M is an elementary abelian p-subgroup of AutS normalised by ψ. Clearly $A_M \leqslant C_{\mathrm{Aut}S}(S/M,M)$,, so if $\mu_x \in A_M \cap \mathrm{Inn}S$ then x lies in $C_S(M) = Z(M)$.

Our aim is to show that if (S,ψ) is admissible then A_M lies in InnS. Before doing so we introduce some notation and prove a lemma.

Let b be an element of S which does not lie in M. Then $S = \langle b,M \rangle$. Let $X = \langle u \in Z(M) | u^p \in Z(S) \rangle$. X is normal in S and is normalised by ψ. X lies in $Z(M)$ so X is abelian, and $\Omega_1 X$ is just F. We are going to associate three homomorphisms with X.

The map $q : x \longrightarrow x^p$ for all $x \in X$ is a group homomorphism as X is abelian, and $Xq \leq Z(S)$. $\mathrm{Ker} q = \Omega_1 X = F$. q is a ψ-homomorphism as $xq\psi = x^p\psi = (x\psi)^p = x\psi q$ for all $x \in X$.

The map $\gamma : X \longrightarrow X$ defined by $x\gamma = [b,x]$ for all $x \in X$ is a homomorphism as $[b,xy] = [b,x]^y[b,y] = [b,x][b,y]$ for all x,y in X as X is abelian. $\mathrm{Ker}\gamma = C_X(b)$ which is just $Z(S)$ as $Z(S) \leq X \leq Z(M)$; thus $\mathrm{Ker}\gamma \geq Xq$. If $x \in X$ then $(x\gamma)^p = [b,x]^p = [b,x^p] = 1$ as $x^p \in Z(T)$ so $\mathrm{Ker}q \geq X\gamma$.

As X is abelian the map $\jmath : x \longrightarrow x^{1+b \ \cdots \ +b^{p-1}}$ for all $x \in X$ is a homomorphism. $x\jmath\gamma = x\gamma\jmath = (x^{-1}.x^b)^{1+b \ \cdots \ +b^{p-1}} = x^{-1}\jmath.x\jmath = 1$ (as b^p centralises x) so $\mathrm{Ker}\jmath \geq X\gamma$ and $Z(T) = \mathrm{Ker}\gamma \geq X\jmath$. ψ is a p-automorphism of S and ψ stabilises S/M so ψ centralises S/M and $b\psi = bs$ for some $s \in M$. Thus $(x\psi)\jmath = (x\psi)^{1+b \ \cdots \ +b^{p-1}} = (x^{1+b \ \cdots \ +b^{p-1}})\psi = (x\jmath)\psi$ for all x in X and $\jmath$ is a ψ-homomorphism.

4.1.1 <u>Lemma</u> Using the notation established above

1) $A_M/A_M \cap \mathrm{Inn}S$ is isomorphic to $\mathrm{Ker}\jmath|_F/X\gamma$.

2) If Xq contains $Z(S)$ then $A_M \leq \mathrm{Inn}S$.

3) If $A_M \leq \mathrm{Inn}S$ then $\Omega_1(Z(S)) \leq S'$. If further $\Omega_1(Z(M))$ contains no free $K(S/M)$ submodule then $Z(S) \leq \mho_1(Z(M))$ and $F = \Omega_1(Z(M)) \leq S'$.

<u>Proof</u> 1) Define $\Delta : A_M \longrightarrow F$ by $\Delta : \beta \longrightarrow b^{-1}.b\beta$ for all $\beta \in A_M$. Given η, θ in F then $(\eta\theta)\Delta = b^{-1}.b\eta\theta = (b^{-1}.b\eta)(b\eta)^{-1}b\eta\theta = (b^{-1}.b\eta)(b^{-1}.b\theta) = \eta\Delta.\theta\Delta$ so Δ is a homomorphism. If $u \in F$ then $u \in \mathrm{Im}\Delta \Leftrightarrow \sigma : b \longrightarrow bu$, $\sigma|_M = 1_M$ is an automorphism of $S \Leftrightarrow (bu)^p = b^p \Leftrightarrow u\jmath = 1 \Leftrightarrow u \in \mathrm{Ker}\jmath|_F$.

If $u \in \operatorname{Ker} \mathcal{J}|_F$ then the element σ of A_M corresponding to u will be inner, conjugation by $d \in S$ say, if and only if $m^d = m$ for all $m \in M$ and $b^d = bu$. This happens

$\Longleftrightarrow d \in C_S(M) = Z(M)$ and $u = [b,d] \in F$

$\Longleftrightarrow d \in Z(M)$ and $1 = u^p = [b,d]^p = [b,d^p]$

$\Longleftrightarrow d \in Z(M)$ and $d^p \in C_{Z(M)}(b) = Z(T)$

$\Longleftrightarrow d \in X$

$\Longleftrightarrow u = [b,d] = d\gamma \in X\gamma$.

Thus the image of $A_M \cap \operatorname{Inn} S$ under the isomorphism $\Delta : A_M \longrightarrow \operatorname{Ker} \mathcal{J}|_F$ is $X\gamma$, and so $A/A_M \cap \operatorname{Inn} S$ is isomorphic to $\operatorname{Ker} \mathcal{J}|_F / X\gamma$.

2) Suppose that $Xq \geqslant Z(S)$. Then since in any case $Z(S) \geqslant Xq$, we have $Xq = Z(S) = \operatorname{Ker} \gamma$. $\operatorname{Ker} q \geqslant X\gamma$ and since $|X|/|\operatorname{Ker} q| = |Xq| = |\operatorname{Ker} \gamma| = |X|/|X\gamma|$ we see that $X\gamma = \operatorname{Ker} q = F$. But then we have $F \geqslant \operatorname{Ker} \mathcal{J}|_F \geqslant X\gamma = F$ so $X\gamma = \operatorname{Ker} \mathcal{J}|_F$ and we see from (1) that $A_M \leqslant \operatorname{Inn} S$.

3) If $A_M \leqslant \operatorname{Inn} S$ then $\operatorname{Ker} \mathcal{J}|_F = X\gamma = [b,X] \leqslant S'$.
$\Omega_1(Z(S))$ lies in F, and if $u \in \Omega_1(Z(S))$
$u\mathcal{J} = u^{1+b \; \cdots \; +b^{p-1}} = u^p = 1$, so $\Omega_1(Z(S)) \leqslant \operatorname{Ker} \mathcal{J}|_F \leqslant S'$.
If F contains no free $K(S/M)$ submodule then each indecomposable $K(S/M)$ direct summand has b-height at most $p-1$. This means that if $x \in F$, $1 = x^{(1-b)^{p-1}}$. Now

$(1-b)^{p-1} = \sum_{r=1}^{p-1} (-1)^r \binom{p-1}{r} b^r \equiv \sum_{r=1}^{p-1} b^r \pmod p$ since $(-1)^r \binom{p-1}{r} \equiv 1 \pmod p$

as may be deduced from Wilson's theorem. Hence

$1 = x^{(1-b)^{p-1}} = x^{1+\dots\, b^{p-1}} = x$ so $F\mathcal{J} = 1$ and $F \leqslant \operatorname{Ker} \mathcal{J}|_F$.

Since $\operatorname{Ker} \mathcal{J}|_F = X\gamma$ we see $F = X\gamma \leqslant S'$. Now $\operatorname{Ker} q = F = X\gamma$ and in any case $Z(S) = \operatorname{Ker} \gamma \geqslant Xq$ so $Xq = \operatorname{Ker} \gamma = Z(S)$. Since $Xq \leqslant \mho_1(Z(M))$ the result is proved.

We are now in a position to prove

4.1.2 **Theorem** Let (T,ϕ) be an admissible pair and let N be a maximal subgroup of T which is normalised by ϕ and contains $Z(T)$. Then $A_N \leqslant \mathrm{Inn}T$ where A_N is as defined above.

Proof Let $A_N = A$. Suppose that A does not lie in $\mathrm{Inn}T$. As we remarked above A is normalised by ϕ and A is an elementary abelian p-subgroup of $\mathrm{Aut}T$. We can apply 3.3.9 to deduce that there exists some $\beta \notin A \cap \mathrm{Inn}T$ such that if $[\phi,\beta] = \mu_y \in A \cap \mathrm{Inn}T$ then $Z(T)$ is generated as a $\mathbb{Z}\langle\phi\rangle$ module by $v.v\beta. \ \ldots \ v\beta^{p-1}$ where v is some element of T which is congruent to y modulo $Z(T)$. As $\mu_y \in A \cap \mathrm{Inn}T$ y and hence v lie in $Z(N)$. β centralises N so $v\beta = v$, and $Z(T)$ is generated as a $\mathbb{Z}\langle\phi\rangle$ module by v^p and so $Z(T) \leqslant \mho_1(Z(N))$. But then (2) of the previous lemma shows that $A \leqslant \mathrm{Inn}T$, and we reach a contradiction. Thus $A \leqslant \mathrm{Inn}T$.

Although we will examine the consequences of this theorem in more detail later, there are some deductions which we can make immediately.

4.1.3 **Corollary** Suppose (T,ϕ) is admissible. Then

1) $\Omega_1(Z(T)) \leqslant T'$.

2) If N is a maximal and ϕ-invariant subgroup of T containing $Z(T)$ then either $\Omega_1(Z(N))$ contains a free $K(T/N)$ submodule or $\Omega_1(Z(N)) \leqslant T'$ and $Z(T) \leqslant \mho_1(Z(N))$.

Proof We apply (3) of lemma 4.1.1 with $S = T$, $M = N$ and $\psi = \phi$, since the theorem shows that $A_N \leqslant \mathrm{Inn}T$.

We can use this to construct some outer automorphisms.

4.1.4 **Theorem** Let G be a finitely generated nilpotent group with Hirsch length one whose torsion subgroup T is a non-trivial p-group satisfying one of the following. Then G has a non-inner automorphism acting nilpotently.

a) T has an abelian direct factor

b) $\Omega_1(Z(T))$ is not contained in T'

c) T has exponent p .

Proof Suppose that G has no non-inner automorphisms acting nilpotently. Let $\phi \in \mathrm{Aut}T$ be induced by conjugation by a generator of G/T . Then the argument of 3.3.3 allows us to assume that (T,ϕ) is admissible.

a) If $T = A \times B$ where A is abelian and non-trivial then $Z(T) = A \times Z(B)$ and $Z(A) \cap T' = Z(A) \cap A' = 1$, so $\Omega_1(Z(T)) \nleq T'$ and a) is a special case of b).

b) If (T,ϕ) is admissible then 4.1.3 shows that $\Omega_1(Z(T)) \leq T'$ and the result follows.

c) Let N be a maximal and ϕ-invariant subgroup of T which contains $Z(T)$. Then 4.1.3 shows that either $\Omega_1(Z(N))$ contains a free $K(T/N)$ submodule or $\mho_1(Z(N)) \geq Z(T)$. Now since T has exponent p, $\mho_1(Z(N)) = \langle x^p \mid x \in Z(N) \rangle$ is just the identity so the second possibility cannot hold as otherwise we would have $T = Z(T) = 1$. So $\Omega_1(Z(N))$ contains a free indecomposable direct summand U generated as a $K(T/N)$ module by u say. Let bN be a generator of T/N . Then as T has exponent p, $1 = (bu)^p = b^p u^{1+b} \cdots {}^{+b^{p-1}} = 1.u\mathcal{J}$ where $\mathcal{J}$ is the trace map associated with b . and so $U\mathcal{J} = 1$. But then as U is free our remarks in section 3.3 show that $C_U(b) = 1$, which is impossible. Hence such an admissible pair cannot exist , and so G has a non-inner automorphism acting nilpotently.

Section 4.2

We define the rank of a finitely generated abelian group to be the number of factors in any decomposition of the group as a direct product of cyclic factors. Let T be a finite p-group. In this section we are going to analyse a particular group of central automorphisms of T, and hence obtain information about the rank of the second central factor of an admissible p-group.

Let $E = \Omega_1(Z(T))$ and suppose that $E \leq \Phi(T)$. Let $H = \{\alpha \in \mathrm{Aut}T \mid t^{-1}.t\alpha \in E \ \forall\, t \in T\}$. H is an elementary abelian p-subgroup of $\mathrm{Aut}T$; to show this we will apply 4.0.1 with $B = E$ and $A = \Phi(T)$. We need to show that if $\alpha \in H$ then $\alpha|_{\Phi(T)} = 1$. But $\Phi(T) = T'.\mho_1(T)$ and it is easy to see that $\alpha|_{T'} = 1_{T'}$ and $\alpha|_{\mho_1(T)} = 1_{\mho_1(T)}$.

If $\mu_d \in H \cap \mathrm{Inn}T$ then $g^{-1}.g^d \in E$ for all $g \in G$ and $d \in Z_2(T)$. μ_d has order p so $d^p \in Z(T)$ and $dZ(T) \in \Omega_1(Z_2(T)/Z(T))$. Under the isomorphism of $\mathrm{Inn}T$ and $T/Z(T)$ $H \cap \mathrm{Inn}T$ corresponds to $\Omega_1(Z_2(T)/Z(T))$.

Let $D = T/\Phi(T)$. Then 4.0.1 shows that $H \cong \mathrm{Der}_K(D,E)$ where K is the field of p elements. D acts trivially on E as E is a subgroup of $Z(T)$ so $\theta \in \mathrm{Der}_K(D,E)$ if and only if $(ab)\theta = (a\theta)^b.b\theta = a\theta.b\theta$ for all a,b in D, that is if and only if $\theta \in \mathrm{Hom}_K(D,E)$, and so $\mathrm{Der}_K(D,E) = \mathrm{Hom}_K(D,E)$ and $H \cong \mathrm{Hom}_K(D,E)$.

It is well known that $D^* \otimes_K E \cong \mathrm{Hom}_K(D,E)$, where D^* denotes the vector space dual of D, under the map $\Gamma : \alpha \otimes \beta \longrightarrow \alpha\circ\beta \in \mathrm{Hom}_K(D,E)$ where $\alpha\circ\beta$ is defined by $(d)\alpha\circ\beta = d\alpha.\beta$ for $\alpha \in D^*$ and $\beta \in E$. Thus $H \cong D^* \otimes_K E$.

Now suppose that ϕ is an automorphism of T of p-power order. Then H and $\mathrm{Der}_K(D,E) = \mathrm{Hom}_K(D,E)$ are isomorphic as $K\langle\phi\rangle$ modules, where if $\gamma \in \mathrm{Hom}_K(D,E)$ γ^ϕ is defined so as to make the following diagram commute.

$$\begin{tikzcd} D \arrow[r, "\phi"] \arrow[d, "\gamma"'] & D \arrow[d, "\gamma^\phi"] \\ E \arrow[r, dashed, "\phi"'] & E \end{tikzcd}$$

We want to show that $\Gamma : D^* \otimes_K E \longrightarrow \mathrm{Hom}_K(D,E)$ is a $K\langle\phi\rangle$ isomorphism where $D^* \otimes_K E$ is a $K\langle\phi\rangle$ module under the diagonal action $(\alpha\otimes\beta)\phi = \alpha\phi \otimes \beta\phi$ for all $\alpha\otimes\beta \in D^*\otimes E$, and the $K\langle\phi\rangle$ module structure of D^* is as defined in 3.3.

4.2.1 <u>Lemma</u> $D^*\otimes_K E$ is $K\langle\phi\rangle$ isomorphic to $\mathrm{Hom}_K(D,E)$.

<u>Proof</u> Let $\alpha\otimes\beta \in D^*\otimes_K E$. We need to show that $((\alpha\otimes\beta)\Gamma)^\phi = ((\alpha\otimes\beta)\phi)\Gamma$, that is that $(\alpha\circ\beta)^\phi = (\alpha\phi\otimes\beta\phi)\Gamma = \alpha\phi\circ\beta\phi$. Now if $x \in D$ and $\gamma \in \mathrm{Hom}_K(D,E)$ then $x.\gamma^\phi = x\phi^{-1}\gamma\phi$ so

$$\begin{aligned} x(\alpha\circ\beta)^\phi &= x\phi^{-1}.\alpha\circ\beta.\phi = \{(x\phi^{-1})\alpha.\beta\}\phi \\ &= (x\phi^{-1})\alpha.\beta\phi \qquad (\text{as } (x\phi^{-1})\alpha \in K) \\ &= x(\alpha\phi).\beta\phi \qquad \text{by the definition of } (\alpha\phi). \\ &= x(\alpha\phi\circ\beta\phi) \qquad \text{and the result follows.} \end{aligned}$$

Summarising our results so far we have

4.2.2 <u>Lemma</u> Let T be a finite p-group with $\Omega_1(Z(T)) \leq \Phi(T)$ and let ϕ be an automorphism of T of p-power order. Then $H = \{\alpha \in \mathrm{Aut}T \mid t^{-1}.t\alpha \in \Omega_1(Z(T))\ \forall\ t \in T\}$ is $K\langle\phi\rangle$ isomorphic to $D^*\otimes_K E$ and $H \cap \mathrm{Inn}T$ is $K\langle\phi\rangle$ isomorphic to $\Omega_1(Z_2(T)/Z(T))$.

<u>Proof</u> The first isomorphism follows from the previous lemma, the second from our earlier remarks and the fact that the isomorphism between $\mathrm{Inn}T$ and $T/Z(T)$ is obviously a ϕ-map.

To continue we need some information about the ϕ-height of the $K\langle\phi\rangle$ module $D^*\otimes_K E$ in terms of the ϕ-heights of D and E.

4.2.3 Lemma Let F be a cyclic p-group, $F = \langle f\rangle$ say. Suppose U and V are KF modules, where K is the field of p elements, of f-heights u and v respectively. Let $U\otimes_K V$ be a KF module under the diagonal action. Then $U\otimes_K V$ has f-height at most $u+v-1$.

Proof Given non-negative integers i and j define
$R_{ij} = \{ \sum_{r,s} a_{rs}m_r(1-f)^i\otimes n_s(1-f)^j \mid r,s \in \mathbb{N}, m_r \in U, n_s \in V, a_{rs} \in K\}$.
R_{ij} is a $K\langle f\rangle$ submodule of $U\otimes_K V$. $R_{00} = U\otimes_K V$ and $R_{gh} \leqslant R_{st}$ if $g \geqslant s$ and $h \geqslant t$. Given any $a \in U$ then $a(1-f)^u = 0$. Since U has f-height u there exists $a_0 \in U$ such that $a_0(1-f)^{u-1} \neq 0$. Similarly $b(1-f)^v = 0$ for all $b \in V$ and there exists $b_0 \in V$ such that $b_0(1-f)^{v-1} \neq 0$. This shows that $R_{ij} \neq 0$ if and only if $i \leqslant u-1$ and $j \leqslant v-1$. For if $i \leqslant u-1$ and $j \leqslant v-1$ then $0 \neq a_0(1-f)^{u-1}\otimes b_0(1-f)^{v-1} \in R_{(u-1)(v-1)} \leqslant R_{ij}$. Conversely if say $i > u-1$ then any element of R_{ij} is a sum of terms of the form $a(1-f)^i\otimes b(1-f)^j$ for some $a \in U$, $b \in V$ and any such term is zero; similarly if $j > v-1$.

Now for any $a\otimes b \in U\otimes_K V$ we have
$(a\otimes b)(1-f) = a(1-f)\otimes b(1-f) + a(1-f)\otimes bf + af\otimes b(1-f)$ and so it follows that for all non-negative integers i and j
$R_{ij}(1-f) \leqslant R_{(i+1)(j+1)} + R_{(i+1)j} + R_{i(j+1)} = R_{(i+1)j} + R_{i(j+1)}$
since $R_{(i+1)(j+1)} \leqslant R_{(i+1)j}$. Applying this identity and using induction on s we deduce that for all non-negative integers s

$R_{00}(1-f)^s \leqslant \sum_{k=0}^{k=s} R_{k(s-k)}$ since $R_{00}(1-f) \leqslant R_{01} + R_{10}$ and if

$R_{00}(1-f)^s \leqslant \sum_{k=0}^{k=s} R_{k(s-k)}$ then
$$\begin{aligned} R_{00}(1-f)^{s+1} &= R_{00}(1-f)^s(1-f) \\ &\leqslant \left(\sum_{k=0}^{k=s} R_{k(s-k)}\right)(1-f) \\ &\leqslant \sum_{k=0}^{k=s}\left\{R_{(k-1)(s-k)} + R_{k(s-k-1)}\right\} \\ &= \sum_{k=0}^{k=s+1} R_{k(s+1-k)}. \end{aligned}$$

Setting $s = u+v-1$ we see that $R_{00}(1-f)^{u+v-1} = 0$, as given k with $0 \leqslant k \leqslant u+v-1$ either $k \geqslant u$ or $u+v-1-k \geqslant v$ so in either case $R_{k(u-v-1-k)} = 0$. Thus $U \otimes_K V(1-f)^{u+v-1} = 0$ and so $U \otimes_K V$ has f-height at most $u+v-1$.

Let us consider what this tells us about admissible pairs. Let (T,ϕ) be admissible and suppose that $E = \Omega_1(Z(T))$ has order p^e and ϕ-height e' and that $D = T/\Phi(T)$ has order p^d and ϕ-height d'. 4.1.3 shows that $E \leqslant T'$, so E must lie in $\Phi(T)$ and $H = \{\alpha \in \mathrm{Aut}T \mid t^{-1}.t\alpha \in E \ \forall\, t \in T\}$ is an elementary abelian p-subgroup of $\mathrm{Aut}T$ which is normalised by ϕ. 4.2.1 shows that H is $K\langle\phi\rangle$ isomorphic to $D^* \otimes_K E$ and $H \cap \mathrm{Inn}T$ is $K\langle\phi\rangle$ isomorphic to $\Omega_1(Z_2(T)/Z(T))$. As we remarked in section 3.3 D^* and D have the same ϕ-height, and so the previous lemma shows that $D^* \otimes_K E$ and hence H have ϕ-height at most $d'+e'-1$. The order of H is of course p^{de}.

Suppose that H does not lie in $\mathrm{Inn}T$. We can apply 3.3.9 to $H \cap \mathrm{Inn}T$ and we deduce that $H = A.H \cap \mathrm{Inn}T$ where A is a $K\langle\phi\rangle$ indecomposable direct summand of H. Then

$|H| = |A|.|H \cap \mathrm{Inn}T|/|A \cap \mathrm{Inn}T|$ so

$|H||A \cap \mathrm{Inn}T|/|A| = |H \cap \mathrm{Inn}T| = |\Omega_1(Z_2(T)/Z(T))|$. $|H| = p^{de}$ and A is a cyclic submodule of H, which has ϕ-height at most $d'+e'-1$, so $|A| \leqslant p^{d'+e'-1}$. Our next lemma obtains a bound for $|A \cap \mathrm{Inn}T|$, enabling us to estimate the order of $\Omega_1(Z_2(T)/Z(T))$ and hence the rank of the second central factor of T.

4.2.3 **Lemma** Let (T,ϕ) be admissible and suppose that H does not lie in $\mathrm{Inn}T$. Then, using the notation established above

1) $Z(T)$ lies inside $\Phi(T)$.

2) $|A \cap \mathrm{Inn}T| \geqslant p$, and if $e \geqslant 2$ then $|A \cap \mathrm{Inn}T| \geqslant p^2$.

If p is odd or if p is equal to 2 and $\Omega_1(Z(T)) \leqslant \mho_1(Z(T))$ then $|A \cap \mathrm{Inn}T| \geqslant p^e$.

Proof 3.3.9 shows that $Z(T)$ is generated as a $\mathbb{Z}\langle\phi\rangle$ module by $m = v.v\alpha. \ \ldots \ .v\alpha^{p-1}$ where $\alpha \in A$ and $\mu_v = [\phi,\alpha] \in \mathrm{Inn}T$.
$\alpha \in H$ so $v\alpha = va$ for some $a \in \Omega_1(Z(T))$ and $m = v^p a^{\frac{1}{2}p(p-1)}$.

1) It was shown in 4.1.3 that $\Omega_1(Z(T)) \leqslant T'$, so as $v^p \in \mho_1(T)$ and $a^{\frac{1}{2}p(p-1)} \in \Omega_1(Z(T))$ m lies in $\Phi(T) = \mho_1(T).T'$.
$\Phi(T)$ is characteristic in T so $Z(T)$, the $\mathbb{Z}\langle\phi\rangle$ module generated by m, must lie in $\Phi(T)$.

2) Let $\_$ denote images modulo $\mho_1(Z(T))$. Then $\underline{Z(T)}$ is a non-trivial cyclic $K\langle\phi\rangle$ module of order p^e generated by $\underline{m}$. If $|A \cap \mathrm{Inn}T| = 1$ then $v \in Z(T) \leqslant \Phi(T)$ so $v = v\alpha = va$ and $\underline{m} = \underline{v}^p = \underline{1}$ which is impossible as $\underline{Z(T)}$ is non-trivial. Thus $|A \cap \mathrm{Inn}T| \geqslant p$.

In case $|A \cap \mathrm{Inn}T| = p$ then, as $A \cap \mathrm{Inn}T$ is normalised by ϕ, it is centralised by ϕ, so $\mu_v = \mu_v{}^{\phi} = \mu_{v\phi}$ and $v\phi = vu$ for some $u \in Z(T)$. $u\alpha = u$ as $Z(T) \leqslant \Phi(T)$ so $v = v^v = v[\phi,\alpha] = v.a^{-1}.a\phi$ and $a\phi = a$. Thus $\underline{m}\phi = \underline{v^p a^{\frac{1}{2}p(p-1)}}\phi = \underline{mu}^p = \underline{m}$ so as $\underline{Z(T)}$ is generated as a $K\langle\phi\rangle$ module by $\underline{m}$, $\underline{Z(T)}$ has order p and $e = 1$. Thus if $e \geqslant 2$ then $|A \cap \mathrm{Inn}T| \geqslant p^2$.

To prove the final assertion we construct a surjection $\theta : A \cap \mathrm{Inn}T \longrightarrow \underline{Z(T)}$. If $\mu_g \in A \cap \mathrm{Inn}T$ then $g.Z(T) \in \Omega_1(Z_2(T)/Z(T))$ so $g^p \in Z(T)$; we define θ by $\theta : \mu_g \longrightarrow g^p$.

We first observe that if $x \in \Omega_1(Z(T))$ then $\underline{x^{\frac{1}{2}p(p-1)}} = \underline{1}$. For if p is odd $2 | p-1$ and $\underline{x^{\frac{1}{2}p(p-1)}} = \underline{x}^p = \underline{1}$; if p is equal to 2 x lies in $\Omega_1(Z(T)) \leq \mho_1(Z(T))$ so $\underline{x} = \underline{1}$. If $\mu_g, \mu_h \in A \cap \mathrm{Inn}T$ then $(\mu_g \mu_h)\theta = (\mu_{gh})\theta = (\underline{gh})^p = \underline{g^p h^p [g,h]^{\frac{1}{2}p(p-1)}}$. Now $g \in Z_2(T)$ so $[g,h] \in Z(T)$ and $g^p \in Z(T)$ so $1 = [g^p,h] = [g,h]^p$ and $[g,h] \in \Omega_1(Z(T))$.

Thus $(\mu_g \mu_h)\theta = \underline{g}^p \underline{h}^p = \mu_g\theta . \mu_h\theta$ and θ is a homomorphism.

θ is a ϕ-homomorphism since $(\mu_g{}^\phi)\theta = (\mu_{g\phi})\theta = (g\phi)^p = (\mu_g\theta)\phi$ for all $\mu_g \in A \cap \mathrm{Inn}T$. This shows that θ is surjective, since $Z(T)$ is generated as a $K\langle\phi\rangle$ module by $\underline{m} = \underline{v^p a^{\frac{1}{2}p(p-1)}} = \underline{v}^p = \mu_v\theta$ (as $a \in \Omega_1(Z(T))$). Hence $|A \cap \mathrm{Inn}T| \geq |\mathrm{Im}\theta| = |\underline{Z(T)}| = |Z(T) : \mho_1(Z(T))| = |\Omega_1(Z(T))| = p^e$.

4.2.4 **Corollary** Suppose that (T,ϕ) is admissible. Then $Z(T)$ lies in $\Phi(T)$.

Proof Suppose that $Z(T)$ does not lie in $\Phi(T)$ and choose u , an element of $Z(T) \setminus \Phi(T)$. We may pick a generating set $\{u\Phi(T), t_1\Phi(T), \ \ldots \ , t_r\Phi(T)\}$ for $T/\Phi(T)$: then $\{u, t_1, \ \ldots \ , t_r\}$ generate T . Pick $v \in \Omega_1(Z(T)) \leq \Phi(T)$. The map $\alpha : u \longrightarrow uv$, $\alpha : t_i \longrightarrow t_i$ for all $1 \leq i \leq r$ is an automorphism of T and lies in H , where H is defined as above. α acts non-trivially on $Z(T)$ so α can not be inner. Thus H does not lie in $\mathrm{Inn}T$. But then the previous theorem shows that $Z(T) \leq \Phi(T)$, which contradicts our original hypothesis and so the result is proved.

4.2.3 enables us to say something about the rank of $Z_2(T)/Z(T)$.

4.2.5 **Theorem** Let (T,ϕ) be an admissible pair. Let $D = T/\Phi(T)$ have order $p^d > p$ and ϕ-height $d' \geq 1$.

Let $E = \Omega_1(Z(T))$ have order $p^e > 1$ and ϕ-height $e' \geq 1$.

Then <u>either</u>

a) $Z_2(T)/Z(T)$ has rank de <u>or</u>

b) i) If p is odd or $p = 2$ and $\Omega_1(Z(T)) \leq \mho_1(Z(T))$ then $de > \text{rank } Z_2(T)/Z(T) \geq de+e-e'-d'+1$.

ii) In any case

$$de > \text{rank } Z_2(T)/Z(T) \geq de-e'-d'+3 \quad \text{if } e > 1$$

$$d > \text{rank } Z_2(T)/Z(T) \geq d-d'+1 \quad \text{if } e = 1 .$$

<u>Proof</u> Let H be defined as above. Then $H \cap \mathrm{Inn}T \cong \Omega_1(Z_2(T)/Z(T))$ and $Z_2(T)/Z(T)$ has rank x if and only if $|H \cap \mathrm{Inn}T| = p^x$.
Thus H lies in $\mathrm{Inn}T$ whenever $Z_2(T)/Z(T)$ has rank de .

If H does not lie in $\mathrm{Inn}T$ then we may choose A as before. Then $p^{de} > |H \cap \mathrm{Inn}T| = |H||A \cap \mathrm{Inn}T|/|A| \geq p^{de}.|A \cap \mathrm{Inn}T|/p^{d'+e'-1}$ since $H = p^{de}$ and, as we remarked before, $|A| \leq p^{d'+e'-1}$.

i) If p is odd or, $p = 2$ and $\Omega_1(Z(T)) \leq \mho_1(Z(T))$, then 4.2.3 shows that $|A \cap \mathrm{Inn}T| \geq p^e$ so $|H \cap \mathrm{Inn}T| \geq p^{de}.p^e/p^{d'+e'-1}$ and $de > \text{rank } Z_2(T)/Z(T) \geq de+e-e'-d'-1$.

ii) In any case $|A \cap \mathrm{Inn}T| \geq p^2$ if $e > 1$, and $|A \cap \mathrm{Inn}T| \geq p$ if $e = 1$ so substituting for $|A \cap \mathrm{Inn}T|$ in the expression above gives the required results. If $e > 1$ then
$|H \cap \mathrm{Inn}T| \geq p^{de}.p^2/p^{d'+e'-1} = p^{de-e'-d'+3}$ and if $e = 1$ then $e' = 1$ and $|H \cap \mathrm{Inn}T| \geq p^d.p/p^{d'} = p^{d-d'+1}$.

Section 4.3

The object of this section is to show that if (T,ϕ) is admissible then T cannot be an exceptional two group. This is proved by direct calculations of a somewhat routine nature.

Let $\langle x\rangle \cong C_{2^m}$. Then $\mathrm{Aut}\langle x\rangle \cong C_{2^{m-2}} \times C_2$ when $m > 2$ and $\gamma : x \longrightarrow x^5$ is a generator of order 2^{m-2} and $\delta : x \longrightarrow x^{-1}$ is a generator of order 2. Following chapter 5 of [4] we make the following definitions. Given $m > 2$ define

$D_m = \langle x,y \mid x^{2^{m-1}} = y^2 = 1 \;,\; x^y = x^{-1} \rangle$, the dihedral group of order 2^m. $D_m/\langle x\rangle$ acts on $\langle x\rangle$ as $\langle\delta\rangle \leq \mathrm{Aut}\langle x\rangle$. Define

$Q_m = \langle x,y \mid x^{2^{m-2}} = y^2 \;,\; y^4 = 1 \;,\; x^y = x^{-1} \rangle$, the generalised quaternion group of order 2^m. $Q_m/\langle x\rangle$ again acts as $\langle\delta\rangle \leq \mathrm{Aut}\langle x\rangle$ but D_m is a split extension of $\langle x\rangle$ and Q_m is not. Given $m > 3$ define

$S_m = \langle x,y \mid x^{2^{m-1}} = y^2 = 1 \;,\; x^y = x^{-1+2^{m-2}} \rangle$, the semidihedral group of order 2^m. $S_m/\langle x\rangle$ acts on $\langle x\rangle$ as $\langle \gamma^{2^{m-3}}.\delta\rangle \leq \mathrm{Aut}\langle x\rangle$.

If T is a dihedral, generalised quaternion or semidihedral group we say T is exceptional. It is well known (see e.g. [4]) that the exceptional groups are the only non-abelian 2-groups of maximal class. In this section we want to show that if T is an exceptional 2-group and if ϕ is an automorphism of T of 2-power order then (T,ϕ) cannot be admissible. Our first task is to calculate $\mathrm{Aut}T$.

It is well known that $\mathrm{Aut}D_3 \cong D_3$ where $\mathrm{Out}D_3 = \langle \alpha.\mathrm{Inn}D_3\rangle \cong C_2$ where $x\alpha = x$, $y\alpha = yx$; then $\alpha^2 = \mu_x$. $\mathrm{Aut}Q_3 \cong \Sigma_4$ and $\mathrm{Out}Q_3 = \langle \alpha.\mathrm{Inn}Q_3, \beta.\mathrm{Inn}Q_3\rangle \cong \Sigma_3$ where α and β are defined by

$x\alpha = xy$, $y\alpha = y$ and $x\beta = y$, $y\beta = x$.

So let T be an exceptional 2-group of order $2^m > 8$ such that $C_{2^{m-1}} \cong \langle x \rangle = H \lhd T$ and $T/H = \langle yH \rangle \cong C_2$. Then let $x^y = x^{-1+2^k}$ where $k = m-1$ or $m-2$ and let $y^2 = x^{2^{m-2}.r}$ where $r \in \{1,2\}$. The values of r and k are given by

D_m : $r = 2, k = m-1$.

Q_m : $r = 1, k = m-1$.

S_m : $r = 2, k = m-2$.

Now $T' = \langle x^{-1}.x^y \rangle = x^{-2+2^k} = \langle x^2 \rangle$ and $C_T(T') = C_T(x^2) = H$ since $(x^2)^y = x^{-2+2^{k+1}} = x^{-2} \neq x^2$ as x has order $2^{m-1} > 4$. Thus H is characteristic in T so if α is an automorphism of T then $x\alpha = x^i$ for some odd integer i and $y\alpha = yx^j$ for some integer j . Obviously $x\alpha$ has order 2^{m-1} .

$(x\alpha)^{y\alpha} = (x^i)^{yx^j} = (x^i)^y = (x^y)^i = (x^y)\alpha$, and α is a bijection and so α is an automorphism if and only if it preserves the third relation of T , that is if and only if $y^2\alpha = (y\alpha)^2$ that is if and only if $y^2 = yx^jyx^j = y^2.x^{j(-1+2^k+1)}$, if and only if $x^{j.2^k} = 1$. Thus α is an automorphism for all values of i and j if T is isomorphic to D_m or Q_m , and α is an automorphism for all values of i and all even values of j if T is isomorphic to S_m .

The above shows that AutT contains subgroups

$U = \{\alpha \in \mathrm{Aut}T \mid x\alpha = x\} = C_{\mathrm{Aut}T}(H)$ and

$V = \{\theta \in \mathrm{Aut}T \mid y\theta = y\}$ with the following properties.

$U = \langle \beta \rangle$ where $y\beta = yx$ and $U \cong C_{2^{m-1}}$ if $T \cong Q_m$ or D_m and

$y\beta = yx^2$ and $U \cong C_{2^{m-2}}$ if $T \cong S_m$.

Since $U = C_{\mathrm{Aut}T}(H)$, U is normal in AutT .

V is isomorphic to AutH so $V \cong C_{2^{m-2}} \times C_2$. If $\sigma \in V$ is such that $x\sigma = x^i$ then $\beta^\sigma = \beta^i$.

In fact AutT = V.U since if $\alpha \in$ AutT is such that $x\alpha = x^i$ and $y\alpha = yx^j$ then $\alpha = \sigma\beta^j$ if T is isomorphic to D_m or Q_m and $\alpha = \sigma\beta^{\frac{1}{2}j}$ if $T \cong S_m$, where $\sigma \in V$ is such that $x\sigma = x^i$. We remark that in case T is isomorphic to D_m or Q_m AutT is just the holomorph of $C_{2^{m-1}}$; if T is isomorphic to S_m then AutT is isomorphic to the holomorph of $C_{2^{m-1}}$ factored by its centre.

I claim that the exponent of AutT is just the order of U . For let $\sigma\beta^j$ be a typical element of AutT , where $\sigma \in V$, $\beta^j \in U$ and $x\sigma = x^i$ for some $i = 2n+1$. Then

$$(\sigma\beta^j)^{2^{m-2}} = \sigma^{2^{m-2}} . \beta^{j(1+\sigma+\ \dots\ +\sigma^{2^{m-2}-1})}$$

$= \beta^{j.r}$ as V has exponent 2^{m-2} where

$$r = 1+i+\ \dots\ +i^{2^{m-2}-1}$$
$$= j(i^{2^{m-2}}-1)/(i-1)$$
$$= j\{(2n+1)^{2^{m-2}}-1\}/2n$$
$$= j.2^{m-2}.a$$ where a is some odd integer.

Thus $(\sigma\beta^j)^{2^{m-2}} \in \langle\beta^{2^{m-2}}\rangle$, and so AutT has exponent equal to the order of U .

Now InnT = $\langle\mu_x,\mu_y\rangle$. $y\mu_x = yx^2$ so $\mu_x \in U$; $\mu_x = \beta^2$ if T is isomorphic to Q_m or D_m and $\mu_x = \beta$ if T is isomorphic to S_m . In either case V acts trivially on $U/\langle\mu_x\rangle$ so AutT/$\langle\mu_x\rangle$ is abelian, and thus OutT is abelian. $\mu_y \in V$ and is a generator of V of order 2 of V. Thus

AutT/InnT = $V.\langle\beta\rangle/\langle\mu_y\rangle.\langle\beta^2\rangle \cong C_{2^{m-2}} \times C_2$ if $T \cong D_m$ or Q_m and

AutT/InnT = $V.\langle\beta\rangle/\langle\mu_y\rangle.\langle\beta\rangle \cong C_{2^{m-2}}$ if $T \cong S_m$.

These remarks enable us to prove the following theorem

4.3.1 <u>Theorem</u> Let T be an exceptional 2-group and let ϕ be any non-inner element of $\mathrm{Aut}T$ of 2-power order. Then the pair (T,ϕ) is not admissible.

<u>Proof</u> We will consider the different possibilities for T in turn.

Suppose $T \cong D_3$. If (T,ϕ) is admissible then it follows from 3.2.2 that $\langle\phi\rangle \cap \mathrm{Inn}T$ is non-trivial so ϕ must have order 4 and so in the notation given above $\phi \in \{\alpha, \alpha^2\}$. Then $\phi^2 \in \{\mu_x, \mu_{x^3}\}$ and since $x^2 \in Z(T)$ we may assume that $\phi^2 = \mu_x$ and that $c = x$. But then $c\phi = c$, so $[\phi, \langle c, Z(T)\rangle] \not\leq Z(T)$ and (T,ϕ) fails to satisfy part (B) of the definition of an admissible pair.

If $T \cong Q_3$ and (T,ϕ) is admissible then again ϕ has order 4; replacing ϕ by a conjugate if necessary we may assume that $\phi = \beta\mu_x$. Then $\phi^2 = \mu_{yx}$, so without loss of generality $c = yx$. Then $c\phi = xyx^2 = yx = c$, and as in the previous case we obtain a contradiction.

If T is isomorphic to Q_m or D_m with $m > 3$ then $\mathrm{Out}T \cong C_{2^{m-2}} \times C_2$ and so is non-cyclic abelian. Thus if ϕ is an automorphism of T then $2 \,\big|\, |C_{\mathrm{Out}T}(\bar\phi) : \langle\bar\phi\rangle|$. Thus the pair (T,ϕ) fails to satisfy part (A) of the definition of an admissible pair.

Suppose that T is isomorphic to S_m and that $\phi \in \mathrm{Aut}T$. $\mathrm{Out}T$ is cyclic so $C_{\mathrm{Out}T}(\bar\phi)$ is $\mathrm{Out}T$ and if $\langle\bar\phi\rangle$ is a proper subgroup of $\mathrm{Out}T$, (T,ϕ) fails to satisfy part (A) of the definition of an admissible pair. Thus if (T,ϕ) is admissible $\langle\bar\phi\rangle = \mathrm{Out}T$ which is isomorphic to $C_{2^{m-2}}$, and $\langle\mu_c\rangle = \langle\phi\rangle \cap \mathrm{Inn}T = \langle\phi^{2^{m-2}}\rangle$. But $\mathrm{Aut}\,T$ has exponent equal to the order of U, which in this case is 2^{m-2}, so $\phi^{2^{m-2}} = 1 = \mu_c$ and (T,ϕ) cannot be admissible.

Chapter Five When the torsion subgroup has class two

In this chapter we draw together the work of chapters 3 and 4 to produce the main results of this essay. We need one more tool, a knowledge of the ϕ-invariant normal non-cyclic subgroups of a p-group acted on by an automorphism ϕ , and we obtain this in s section 1 as a variant of a well-known result of P.Hall. This result enables us to show that a non-cyclic finitely generated nilpotent group of Hirsch length one whose torsion subgroup is a p-group of odd order with cyclic derived group admits a non-inner automorphism acting nilpotently. This is the first step in the proof that a finitely generated nilpotent group of Hirsch length one whose torsion subgroup has class two admits a non-inner automorphism acting nilpotently. The rest of the proof is given in section two; most of t the work lies in showing that if (T,ϕ) is admissible then T cannot be an extraspecial two group. Section 3 is concerned with a class of p-groups which includes the p-groups of maximal class.

We conclude the chapter and the essay with a summary of our m main results and some naive speculation.

Section 5.1

It is a well-known result due to P.Hall that a finite p-group with no non-cyclic normal subgroups must be cyclic or an exceptional 2-group, and that a finite p-group with no non-cyclic characteristic subgroups must be the central product of subgroups E and R where either $E = 1$ or E is extraspecial and either R is cyclic or $p = 2$ and R is an exceptional 2-group. (See e.g. [4] section5.4) These results classify p-groups P with no non-cyclic subgroups normalised by $\mathrm{Inn}P$, $\mathrm{Aut}P$ respectively. In the next lemma we follow the proof of Hall's result to classify p-groups P admitting an automorphism ϕ of p-power order such that P has no non-cyclic subgroups normalised by $\langle \phi ,\mathrm{Inn}P\rangle$. Of course if ϕ is inner such groups are already classified by Hall's result, and in general the result turns out not to depend on our choice of ϕ , except when P is the dihedral group of order 8.

5.1.1 Lemma Let F be a finite non-abelian p-group, and let q be an automorphism of F of p-power order. Then either $Z_2(F)$ contains a normal and q invariant subgroup isomorphic to $C_p \times C_p$, or F is an exceptional 2-group where, if F is dihedral of order 8 , q is non-inner.

Proof We show first that if F contains L a normal and q invariant subgroup isomorphic to $C_p \times C_p$, then L lies in $Z_2(F)$. For L is normal in F so $|L \cap Z(F)| \geqslant p$. If $|L \cap Z(F)| = p^2$ then $L \leqslant Z(F)$ so of course $L \leqslant Z_2(F)$. If $|L \cap Z(F)| = p$ then $L.Z(F)/Z(F)$ is a normal subgroup of $F/Z(F)$ so $L.Z(F)/Z(F) \cap Z_2(F)/Z(F)$ is non-trivial and since $L.Z(F)/Z(F)$ has order p , $L \leqslant Z_2(F)$.

If q is an automorphism of 2-power order of F, an exceptional 2-group of order at least 16, then F fails to contain a normal subgroup isomorphic to $C_2 \times C_2$ so F cannot contain a normal subgroup of this form which is invariant under q. For a normal subgroup isomorphic to $C_2 \times C_2$ would have to contain a generator of F, and so as F is a two generator group would have to contain a generator of F', which would have order at least 4.

If F is the quaternion group of order 8 then F contains only one element of order 2, so cannot contain any subgroup isomorphic to $C_2 \times C_2$. If F is dihedral of order 8 F contains two normal subgroups isomorphic to $C_2 \times C_2$, but if q is an automorphism of F q normalises either of these if and only if q is inner.

So let F be an arbitrary non-abelian p-group, and let q be an automorphism of F of p-power order. Choose A a subgroup of F which is maximal subject to being abelian, normal and q-invariant. $\Omega_1(A)$ is normal and q-invariant and A_0 the group of automorphisms of $\Omega_1(A)$ induced by q and F has p-power order. If $|\Omega_1(A)| \geqslant p^2$ then there exists a subgroup L of $\Omega_1(A)$ such that $|L| = p^2$ and L is normalised by A_0; then $L \cong C_p \times C_p$ and has the required properties.

Thus we consider the case $|\Omega_1(A)| = p$; that is the case A is cyclic. $C_F(A)$ is normal in F and q-invariant. If $C_F(A)$ strictly contains A then as q is a p-power automorphism of $C_F(A)/A$ we can find $1 \neq uA \in C_F(A) \cap Z(F/A)$ such that $u^{-1}.uq \in A$. Then $\langle u,A \rangle \gneqq A$ and is q-invariant, normal(as $uA \in Z(F/A)$) and abelian (as $u \in C_F(A)$), contradicting the maximality of A. Thus $C_F(A) = A$, so F/A is isomorphic to a p-subgroup H of $\mathrm{Aut}A$ and in particular F/A is abelian.

Since F is non-abelian , F/A and thus H are non-trivial.

I claim q centralises F/A . Let $sA \in F/A$ Then suppose $A = \langle a \rangle$. Let $a^s = a^i$ for some integer i , then $x^s = x^i$ for all x in A . We have $s^{-1}.aq^{-1}.s = (aq^{-1})^i = a^i q^{-1}$ so $(s^{-1}q)a(sq) = (s^{-1}.aq^{-1}.s)q = a^i q^{-1}.q = a^i = a^s$. Thus $sq.s^{-1} \in C_F(A)$ which is just A , so q centralises F/A .

It follows that if uA is a non-trivial element of $\Omega_1(F/A)$ then $L_u = \langle u,A \rangle$ is a normal, non-abelian and q-invariant subgroup of F . L_u is normal as F/A is abelian, so A contains F' , and L_u is not abelian as $A = C_F(A)$. L_u/A has order p; let $A \cong C_{p^r}$. It is easy to classify such L_u ; the proofs are given in e.g.[4] 5.4.4 . If p is odd $L_u = M_{r+1}(p) = \langle x.y \mid x^{p^r} = y^p = 1,\ x^y = x^{1+p^{r-1}} \rangle$; then $\Omega_1(L_u) = C_p \times C_p$. Since L_u is q-invariant and normal so is $\Omega_1(L_u)$ and thus it is the required normal subgroup.

When $p = 2$ and $r \geqslant 3$ then $H \leqslant \mathrm{Aut}A \cong C_{2^{r-2}} \times C_2$. We may take as generators for AutA $\alpha : x \longrightarrow x^5$ for all x in A , and $\beta : x \longrightarrow x^{-1}$ for all x in A . α has order 2^{r-2} , β has order 2 . Let $\alpha^{2^{r-3}} = \gamma$, then $x\gamma = x^{1+2^{r-1}}$. If $|F/A| > 2$ then $\gamma \in H$ and we may choose $uA \in F/A$ such that $x^u = x\gamma$ for all x in A . $L_u \cong M_{r+1}(2)$ and again $\Omega_1(L_u) \cong C_2 \times C_2$ and is normal and q-invariant as required. If $|F/A| = 2$ then F is classified in 5.4.4iii of [4] ; either $F = M_{r+1}(2)$ when $\Omega_1(F)$ has the required form or F is an exceptional 2-group and was discussed in our remarks at the beginning of the proof.

When $p = 2$ and $r = 3$ F is again an exceptional 2-group.

Our main reason for considering this result is that it enables us to prove the following theorem about p-groups with cyclic derived group, which will be used in our analysis of p-groups of class two.

5.1.2 <u>Theorem</u> Let (T,ϕ) be admissible and suppose that T has cyclic derived group. Then T is a 2-group.

<u>Proof</u> Section 4.3 shows that if (T,ϕ) is admissible then T is not an exceptional 2-group. Thus applying the previous lemma with $F = T$ and $q = \phi$ we deduce that there exists a normal and ϕ-invariant subgroup L of T lying in $Z_2(T)$ and isomorphic to $C_p \times C_p$. 4.1.3 shows that as (T,ϕ) is admissible $\Omega_1(Z(T))$ lies in T', so as T' is cyclic $Z(T)$ must be cyclic. This means that L cannot lie in $Z(T)$; since L is normal in T, $L \cap Z(T)$ has order p. Let $\langle u, L \cap Z(T) \rangle = L$ for some u in L. Let $N = C_T(u)$; then $N = C_T(L)$. All conjugates of u lie in L so as $u \notin Z(T)$ u has precisely p conjugates and so $p = |\text{conjugacy class of } u| = |T:C_T(u)| = |T:N|$. Thus N is a maximal subgroup of T. N is ϕ-invariant, as L is, and N is a centraliser so N contains $Z(T)$.

We have produced N so that we can apply (2) of 4.1.3 to it. We deduce that either $\Omega_1(Z(N))$ contains a free $K(T/N)$ module or $\Omega_1(Z(N)) \leq T'$. Now N centralises L and L has exponent p, so $L \leq \Omega_1(Z(N))$. However L is not cyclic so L does not lie in T'. Thus $\Omega_1(Z(N))$ does not lie in T' and so the first possibility holds, and $\Omega_1(Z(N))$ contains a free $K(T/N)$ submodule, and hence a free cyclic $K(T/N)$ submodule U say. If T/N is generated by bN say U has bN- height p, so order p^p and $[b,U]$ has order p^{p-1} as, since U is a cyclic $\langle bN \rangle$ module,

$|U:[b,U]| = p$. As $[b,U]$ has exponent p we see that $[b,U]$ is an abelian subgroup of T' of rank $p-1$. But T' is cyclic, so $p-1 = 1$, that is, $p = 2$.

5.1.3 Corollary Let G be a finitely generated nilpotent group which is not cyclic, and whose torsion subgroup is a p-group with odd order and cyclic derived group. Then G admits a non-inner automorphism acting nilpotently.

Proof We need only consider the case when G has Hirsch length one. If the torsion subgroup of G is abelian then the result follows from 3.2.2. Otherwise, if G has no automorphism of the required form, then T , the torsion subgroup of G , is a non-abelian p-group with cyclic derived group and if ϕ is an automorphism of T induced by conjugation by a generator of G/T then the pair (T,ϕ) is admissible. But this contradicts the previous theorem.

Notice that since metacyclic p-groups have cyclic derived group this shows that a finitely generated nilpotent group whose torsion subgroup is a metacyclic p-group of odd order admits a non-inner automorphism.

Section 5.2

In this section we prove that a finitely generated nilpotent group with at least three elements whose torsion subgroup is of class two admits a non-inner automorphism. We do this by considering an admissible pair (T,ϕ) where T is a p-group of nilpotency class two and ϕ is an automorphism of T of p-power order. We reduce first to the case where $Z(T)$ is cyclic, then deduce that T must be a 2-group and in fact an extraspecial 2-group. We conclude our proof by showing that if T is an extraspecial 2-group then (T,ϕ) cannot be admissible.

Most of this follows fairly directly from what we have done already. However to analyse the extraspecial case we develop a specialised (and lengthy) argument involving computation and induction on the group order.

5.2.1 Theorem Let (T,ϕ) be admissible and suppose that T has nilpotency class two. Then $Z(T)$ is cyclic.

Proof We want to apply 4.2.5 . Let $T/\Phi(T)$ have rank $d \geqslant 2$ and ϕ-height $d' \geqslant 1$. Let $\Omega_1(Z(T))$ have rank $e \geqslant 1$ and ϕ-height $e' \geqslant 1$. As T has class two $Z_2(T) = T$ and T' lies inside $Z(T)$. Thus $\operatorname{rank} Z_2(T)/Z(T) = \operatorname{rank} T/Z(T) \leqslant \operatorname{rank} T/T'$. The rank of T/T' is just the rank of $T/\Phi(T)$ and so $d \geqslant \operatorname{rank} Z_2(T)/Z(T)$.

Now suppose that $Z(T)$ is not cyclic, that is that $e > 1$. 4.2.5 shows that either $de = \operatorname{rank} Z_2(T)/Z(T)$ or $de > \operatorname{rank} Z_2(T)/Z(T) \geqslant de-e'-d'+3$.

As $e > 1$ it follows that $de > d \geqslant \operatorname{rank} Z_2(T)/Z(T)$ and so the second possibility holds. We have

$d \geqslant \operatorname{rank} Z_2(T)/Z(T) \geqslant de-e'-d'+3$

that is $\quad d \geqslant de-e-d+3 \quad$ since $e \geqslant e'$ and $d \geqslant d'$

$$\begin{aligned} \text{so} \qquad 0 &\geqslant (d-1)(e-2)+1 \\ &\geqslant (2-1)(e-2)+1 \qquad \text{as } d \geqslant 2 \\ &= e-1 \end{aligned}$$

and $e \leqslant 1$. But this contradicts our assumption that $e > 1$, so $e = 1$ and $Z(T)$ is cyclic.

Our next step is to reduce to the case where T is a 2-group, and to do this we use the result of the preceding section.

5.2.2 Lemma Let (T,ϕ) be admissible and suppose that T has nilpotency class two. Then T is a 2-group with cyclic centre.

Proof The previous theorem shows that $Z(T)$ is cyclic. As T has class two T' is a subgroup of $Z(T)$ and so is cyclic. We may apply 5.1.2 and we deduce that T is a 2-group.

We recall that a finite p-group is called extraspecial if the centre and derived group are of order p . It follows that the centre and derived group are equal and equal to the Frattini subgroup, and that the central quotient is elementary abelian. A class two p-group whose centre is of order p must be extraspecial since its derived group is non-trivial and a subgroup of the centre. Thus in considering admissible pairs (T,ϕ) where T is a 2-group with cyclic centre we need to consider two cases; those whose centre has order at least 4 and those which are extraspecial.

5.2.3 <u>Lemma</u> Suppose that (T,ϕ) is admissible and that T has nilpotency class 2 . Then T is an extraspecial 2-group.

<u>Proof</u> We know that T is a 2-group and $Z(T)$ is cyclic. Suppose that $Z(T)$ has order $2^n \geqslant 4$. Let $\langle\phi\rangle \cap \mathrm{Inn}T = \langle\mu_c\rangle$ where $\mu_c = \phi^{2^c}$. Let $Z(T) = \langle z\rangle$ say, and let $y = z^{2^{n-2}}$. Then $\langle y\rangle = \Omega_2(Z(T))$ which is characteristic in T so $y\phi = y.y^{2\eta}$ for some $\eta \in \{0,1\}$, and $y\phi^2 = y$. We may assume that T is not an exceptional 2-group (section 4.3) so T contains a normal and ϕ-invariant subgroup $L \cong C_2 \times C_2$. $L \cap Z(T) = \langle y^2\rangle$ and $L = \langle u, y^2\rangle$ for some $u \in L$ with $u^2 = 1$. L is ϕ-invariant so $u\phi = u.y^{2\delta}$ for some $\delta \in \{0,1\}$. As we remarked in the proof of 5.1.2 $C_T(L)$ is a maximal and ϕ-invariant subgroup of T containing $Z(T)$; let $N = C_T(L)$. Let $T = \langle b,N\rangle$ for some $b \in T\setminus N$. ϕ centralises T/N so $b\phi = bd$ for some $d \in N$. u lies in $Z(N)$ but not in $Z(T)$ so $u^b \neq u$ and we must have $u^b = u.y^2$.

We define $\alpha : T \longrightarrow T$ by $\alpha : b \longrightarrow buy$, $\alpha|_N = 1$. $b^2\alpha = buybuy = b^2u^buy^2 = b^2uy^2uy^2 = b^2$ so α is well defined and obviously $\alpha \in \mathrm{Aut}T$. α is not inner as uy is not an element of $Z(T)$ so is not an element of T' . $\alpha^2|_N = 1$ and $b\alpha^2 = buyuy = by^2$ so $\alpha^2 = \mu_u$, and $\bar{\alpha}$ has order 2 in $\mathrm{Out}T$.

We want to show that $\bar{\alpha} \in C_{\mathrm{Out}T}(\bar{\phi})$.

$$\begin{aligned} b[\alpha,\phi] &= b\alpha^{-1}\phi^{-1}\alpha\phi = (b(uy)^{-1})\phi^{-1}\alpha\phi = (b(d^{-1}\phi^{-1})y^{-1}.y^{-2\eta}.u^{-1}y^{-2\delta})\alpha\phi \\ &= (buy(d^{-1}\phi^{-1})y^{-1}u^{-1}.y^{-2\eta}y^{-2\delta})\phi = (b(d^{-1}\phi^{-1})y^{-2(\eta+\delta)})\phi \\ &= b.y^{-2(\eta+\delta)} = b^{u^{-(\eta+\delta)}} . \end{aligned}$$

$$n[\alpha,\phi] = n = n^{u^{-(\eta+\delta)}} \quad \text{for all } n \in N \text{ as } u \in Z(N) .$$

This shows that $[\alpha,\phi]$ is just conjugation by $u^{-(\eta+\delta)}$ so $[\alpha,\phi]$ is inner on T and $[\bar{\alpha},\bar{\phi}] = 1$. Now (T,ϕ) is admissible so it follows from the definition of admissibility that $\bar{\alpha} \in \langle\bar{\phi}\rangle$. $\bar{\alpha}$ has order 2 so $\bar{\alpha} = \bar{\phi}^{2^{s-1}}$ and there exists $t \in T$ such that $\alpha\mu_t = \phi^{2^{s-1}}$. Then

$$\mu_{u^{-(\eta+\delta)}} = [\alpha,\phi] = [\phi^{2^{s-1}}\mu_{t^{-1}},\phi] = [\mu_{t^{-1}},\phi] = \mu_{t.t^{-1}\phi}$$

. Thus $t\phi$ is equal to $u^{\delta+\eta}.t$ modulo $Z(T)$ and so $t\phi = u^{\delta+\eta}.t.z^{\theta}$ for some integer θ.

Now we calculate μ_c.

$$\mu_c = \phi^{2^s} = (\alpha\mu_t)^2 = \alpha\mu_t\alpha\mu_t = \alpha^2\mu_{t\alpha.t} = \mu_{u.t\alpha.t}$$

. Thus as c was only defined modulo $Z(T)$ we may set $c = u.t\alpha.t$. Then

$$\begin{aligned} c\phi &= (u.t\alpha.t)\phi \\ &= u\phi.t\phi\alpha[\alpha,\phi].t\phi \\ &= uy^{2\delta}.(u^{\delta+\eta}.t.z^{\theta})\alpha[\alpha,\phi].(u^{\delta+\eta}tz^{\theta}) \\ &= uy^{2\delta}.(u^{\delta+\eta}.t\alpha.z^{\theta})[\alpha,\phi].(u^{\delta+\eta}tz^{\theta}) \qquad \text{as } \alpha \text{ centralises } N \\ &= uy^{2\delta}.(u^{\delta+\eta}.t\alpha.z^{\theta})u^{-(\eta+\delta)}.u^{\delta+\eta}tz^{\theta} \\ &= uy^{2\delta}.t\alpha.tz^{2\theta} \\ &= c.y^{2\delta}.z^{2\theta} \qquad \text{as } y \in Z(T). \end{aligned}$$

Thus $c^{-1}.c\phi = y^{2\delta}.z^{2\theta}$ which is an element of $\mho_1(Z(T))$. But this contradicts 3.3.3 which showed that if (T,ϕ) is admissible then $Z(T)/\mho_1(Z(T))$ is generated as a $K\langle\phi\rangle$ module by $c^{-1}.c\phi\,.\,\mho_1(Z(T))$. Thus our hypothesis that $Z(T)$ has order at least 4 must be false and T is extraspecial.

The final step in our argument is to show that there cannot exist an admissible pair (T,ϕ) with T an extraspecial 2-group. The proof is rather long but the idea is that we assume T is an extraspecial 2-group admitting an automorphism ϕ of 2-power order such that $\langle\phi\rangle\cap \mathrm{Inn}T \geqslant \langle\mu_c\rangle \neq 1$ for some $c \in T$ and $\langle c^{-1}.c\phi\rangle = Z(T)$, and try to obtain a contradiction. We regard $T/Z(T)$ as a $K\langle\phi\rangle$ module where K is the field of two elements. $T/Z(T)$ is also equipped with a bilinear form and we examine both this and the module structure to discover how ϕ acts on T. Using induction on $|T|$ enables us to assume that the bilinear form has certain properties which make it possible to calculate the action of ϕ on T. This means that we can identify c, and calculating $c^{-1}.c\phi$ we obtain a final contradiction.

5.2.4 __Theorem__ Let T be a 2-group with cyclic centre and let ϕ be an automorphism of T of 2-power order such that $\langle\phi\rangle\cap \mathrm{Inn}T \geqslant \langle\mu_c\rangle \neq 1$ for some c in T with $\mu_c = \phi^{2^s}$ for some $s \geqslant 1$. Suppose that $\langle c^{-1}.c\phi\rangle = Z(T)$. Then T is not extraspecial.

__Proof__ We suppose that T is an extraspecial 2-group satisfying the conditions of the theorem and having minimal order. Then 4.3.1 shows that T is not exceptional, so we may assume $|T| \geqslant 16$. Let $Z(T) = \langle z\rangle \cong C_2$ and let bars denote images modulo $Z(T)$. Then $A = \underline{T}$ is a K vector space (written multiplicatively in this proof) where K is the field of two elements. Any subspace of A can be expressed uniquely in the form $\underline{L}$ for some normal subgroup L of T containing $Z(T)$. Furthermore A is a $K\langle\phi\rangle$ module and if $\underline{L}$ is a $K\langle\phi\rangle$ submodule of A,, L is a ϕ-invariant subgroup of T.

A admits a non-degenerate alternating bilinear form $[\ ,\ ] : A\times A \longrightarrow K$ induced from the commutator homomorphism $[\ ,\ ] : T\times T \longrightarrow Z(T)$. If $\underline{U}$ is a K-subspace of A let

$(\underline{U})^{\perp} = \{\underline{x} \in A \mid [\underline{x}.\underline{U}] = 1\}$. We shall denote by $U^{\perp}$ the subgroup of T such that $\underline{U}^{\perp} = (\underline{U})^{\perp}$; then $U^{\perp} = C_T(U)$. We recall that $(\underline{U})^{\perp\perp} = \underline{U}$ and $\dim_K\underline{U} + \dim_K(\underline{U})^{\perp} = \dim_K A$. If U is a $K\langle\phi\rangle$ submodule of A then so is $\underline{U}^{\perp}$.

Our first step in the proof is to show that if $\underline{U}$ is a non-trivial $K\langle\phi\rangle$ submodule of A and $\underline{U} \cap \underline{U}^{\perp} = 1$ then $\underline{U} = A$. For as $\underline{U} \cap \underline{U}^{\perp} = 1$ $A = \underline{U} \oplus \underline{U}^{\perp}$, and $\underline{c}$ lies in A so $c = ab$ for some $a \in U$, $b \in U^{\perp}$. $c\phi = cz$ so $\underline{c\phi} = \underline{c}$ and thus $\underline{a\phi} = \underline{a}$ and $\underline{b\phi} = \underline{b}$ (as $\underline{U}$ and $\underline{U}^{\perp}$ are ϕ-invariant) . Thus $a\phi = az^{\eta}$ and $b\phi = bz^{\delta}$ for some $\eta, \delta \in \{0,1\}$. So $c\phi = cz^{\eta+\delta}$, and we may assume that $\eta = 1$ and $a\phi = az$, since as $\underline{U}^{\perp\perp} = \underline{U}$ we may replace $\underline{U}$ by $\underline{U}^{\perp}$ if neccessary. Now we consider the group U . $\underline{U} \cap \underline{U}^{\perp} = 1$ so $C_T(U) \cap U = Z(T) = Z(U)$ and U is extraspecial. U is ϕ-invariant, so we can regard ϕ as an element of $\mathrm{Aut}U$. Now ϕ^{2^s} acts on T as $c = ab$, but $b \in U^{\perp} = C_T(U)$ so ϕ^{2^s} acts on U as $a \in U$. Furthermore $a^{-1}.a\phi = z$ where z generates $Z(U) = Z(T)$. Thus we have shown that U is an extraspecial 2-group satisfying the hypotheses of the theorem, so by the minimality of the order of T , $U = T$ and $\underline{U} = A$.

Our next step is to analyse the action of ϕ on certain subgroups of T . $Z(T) \cong C_2$ so ϕ centralises $Z(T)$. We need to look at how the action of ϕ relates to the form $[\ ,\ ]$. If U and V are two subgroups of T then $[U,V] \leq Z(T)$ so $[[U,V],\phi] = 1$. Applying the three subgroup lemma to U , V and $\langle\phi\rangle$ regarded as subgroups of $T \rtimes \langle\phi\rangle$ we deduce that $[[V,\phi]U] = 1$ if and only if $[V,[U,\phi]] = 1$. Since $[[V,\phi]U]$ and $[V,[U,\phi]]$ are subgroups of $Z(T)$ which has order 2 we deduce that $[V,[U,\phi]] = [[V,\phi],U]$ for all subgroups U , V of T .

Applying this result repeatedly shows that if $n \geq 0$

$$[V,[U,\overbrace{\phi,\phi,\ \ldots\ ,\phi}^{n}]] = [[V,\overbrace{\phi,\ \ldots\ ,\phi}^{r}],[U,\overbrace{\phi,\ \ldots\ ,\phi}^{n-r}]] \qquad (1)$$

for all $0 \leq r \leq n$ and for all subgroups U,V of T.

Now let $\underline{W}$ be an indecomposable $K\langle\phi\rangle$ submodule of A with $|\underline{W}| = 2^d$. ϕ^{2^s} acts as an inner automorphism of T so acts trivially on A and $d \leq 2^s$. Let $\underline{W}$ be generated as a $K\langle\phi\rangle$ module by $\underline{a}$ say, for some a in W. Define $a_{i+1} = a_i^{-1}.a_i\phi$. Then $\{\underline{a}_1, \ \ldots\ ,\underline{a}_d\}$ form a K basis for $\underline{W}$, $a_{d+1} \in Z(T)$ and $a_m = 1$ for $m \geq d+2$. We exhibit some properties of the a_i. Let $W_i = \langle a_j \mid j \geq i\rangle$. Then $W_i = [W,\overbrace{\phi,\ .\ .\ ,\phi}^{i-1}]$ and $\underline{W}_i$ is the unique $K\langle\phi\rangle$ submodule of $\underline{W}$ of index 2^{i-1} in $\underline{W}$; $\underline{W} = \underline{W}_1 > \underline{W}_2 > \underline{W}_3 \ \ldots > \underline{W}_{d+1} = 1$. For each j, $a_j^{\,2} \in Z(T) = \langle z\rangle$. ϕ is an automorphism of T and $z\phi = z$ so

$$a_j^{\,2} = a_j^{\,2}\phi = (a_ja_{j+1})^2 = a_j^{\,2}a_{j+1}^{\,2}[a_j,a_{j+1}] \text{ and } a_{j+1}^{\,2} = [a_j,a_{j+1}]$$

for all $j \geq 1$. (2)

I claim that (i) $a_j^{\,2} = 1$ for all $j \geq [d/2]+2$

(ii) if d is even, $d = 2n$ say, then $a_{n+1}^{\,2} = 1$ if and only if $\underline{W} \cap \underline{W}^{\perp} \neq 1$.

To show this we set $U = V = W$ in (1) above. Then $[W_1,W_x] = [W_{k+1},W_{x-k}]$ for all $1 \leq x \leq d+1$, $0 \leq k \leq x$. Now $W_{d+1} \leq Z(T)$ so $[W_1,W_{d+1}] = 1$, so $1 = [W_{k+1},W_{d+1-k}]$ for all $0 \leq k \leq d+1$. Setting $k = [d/2]$ we deduce that $1 = [W_{[d/2]+1},W_{d+1-[d/2]}]$. Now $d+1-[d/2] \geq [d/2]+1$ and $W_i < W_j$ for $j > i$ so $1 = [W_{[d/2]+1},W_{[d/2]+1}]$. Hence if $j \geq [d/2]+1$ then $[a_j,a_{j+1}] = 1$ and (2) shows that $a_j^{\,2} = 1$..

Now we prove (ii). Suppose that d is even, $d = 2n$ say.

Then (2) shows that ${a_{n+1}}^2 = 1$ if and only if $[a_n, a_{n+1}] = 1$. We have $1 = [W_{n+1}, W_{n+1}]$ and so $1 = [a_{n+1}, a_n]$ if and only if $1 = [W_{n+1}, W_n]$. Now $[W_{n+1}, W_n] = [W_1, W_{2n}]$ so $1 = [W_{n+1}, W_n]$ if and only if $[W_1, W_{2n}] = 1$, that is if and only if $\underline{W}_{2n} \leq \underline{W}_1{}^{\perp}$. Now since $\underline{W}_1$ is a $K\langle\phi\rangle$ submodule of A, $\underline{W}_1 \cap \underline{W}_1{}^{\perp}$ is a $K\langle\phi\rangle$ submodule of $\underline{W}_1$ so is non-trivial if and only if it contains $\underline{W}_{2n}$. Thus ${a_{n+1}}^2 = 1$ if and only if $\underline{W}^{\perp} \cap \underline{W} \neq 1$.

Our next task is to calculate the action of ϕ^{2^s} on W. I claim that for all $i \geq 1$, $k \geq 1$

$a_i\phi^{2^k} = a_i a_{i+2^k} \cdot a^2_{i+2^{k-1}} \cdot {}_iu_k$ where ${}_iu_k \in \langle a_f^2 \mid f > i+2^{k-1} \rangle$. Note that ${}_iu_k \in Z(T)$ so is centralised by ϕ. The proof is by induction on k. For $k = 1$ we have

$$
\begin{aligned}
a_i\phi^2 &= (a_i a_{i+1})\phi \\
&= a_i a_{i+1} \cdot a_{i+1} a_{i+2} \\
&= a_i a_{i+2} {a_{i+1}}^2 \quad \text{as required.}
\end{aligned}
$$

Suppose that $a_i\phi^{2^k} = a_i \cdot a_{i+2^k} \cdot a^2_{i+2^{k-1}} \cdot {}_iu_k$. Then $a_i\phi^{2^{k+1}} =$

$$
\begin{aligned}
&a_i \cdot a_{i+2^k} \cdot a^2_{i+2^{k-1}} \cdot {}_iu_k \cdot a_{i+2^k} \cdot a_{i+2^k+2^k} \cdot a^2_{i+2^k+2^{k-1}} \cdot {}_{i+2^k}u_k \cdot a^2_{i+2^{k-1}} \cdot {}_iu_k \\
&= a_i \cdot a_{i+2^{k+1}} \cdot a^2_{i+2^k} \cdot {}_{i+2^k}u_k \cdot a^2_{i+2^k+2^{k-1}} .
\end{aligned}
$$

Now ${}_{i+2^k}u_k \in \langle a_f^2 \mid f > i+2^k+2^{k-1} \rangle$ so ${}_{i+2^k}u_k \cdot a^2_{i+2^k+2^{k-1}} \in \langle a_f^2 \mid f > i+2^k \rangle$ as required.

In particular this shows us that

$a_i\phi^{2^s} = a_i \cdot a_{i+2^s} \cdot a^2_{i+2^{s-1}} \cdot {}_iu_{2^s}$ where ${}_iu_{2^s} \in \langle a_j^2 \mid j > i+2^{s-1} \rangle$. Now $d \leq 2^s$ so $[d/2] \leq 2^{s-1}$ and $[d/2] + 2 \leq 2^{s-1} + i+1$. Thus if $j \geq 2^{s-1}+i+1$, (i) shows that $a_j^2 = 1$. It follows that ${}_iu_{2^s}$ is always 1. In fact $[d/2] + 2 \leq 2^{s-1} + i$ unless $i = 1$ and $d = 2^s$, so applying (i) again we see $a^2_{i+2^{s-1}} = 1$ unless $i = 1$ and $d = 2^s$. We have now calculated the action of ϕ on

W . We have $a_i\phi^{2^s} = a_i . a_{i+2^s} . a^2_{i+2^{s-1}}$ if $i = 1$ and $d = 2^s$ and $a_i\phi^{2^s} = a_i . a_{i+2^s} = a_i$ otherwise (since then $2^s+i > d+1$ and $a_{i+2^s} = 1$). (3)

Having looked at the action of ϕ on one submodule of $\underline{A}$ we now consider a $K\langle\phi\rangle$ decompostion of $\underline{A}$. Let $\underline{A} = \bigoplus_{i=1}^{t} \underline{X}_i$ be a decomposition of $\underline{A}$ into a direct sum of indecomposable $K\langle\phi\rangle$ submodules. ϕ^{2^s} acts non-trivially on T so must act non-trivially on some X_i . Let X_i be W in the argument above. Then $d = 2^s$ and $a_1\phi^{2^s} = a_1 . a_{1+2^s} . a^2_{1+2^{s-1}} \neq a_1$, and so $a_{1+2^s} . a^2_{1+2^{s-1}} \neq 1$. We now consider two cases, first the case $W = T$ and second the case $W \neq T$.

Suppose that $W = T$. Then $\underline{W} = A$ and $\underline{W} \cap \underline{W}^{\perp} = 1$. By (ii) $a^2_{1+2^{s-1}} \neq 1$, so $a_{1+2^s} = 1$. Now ϕ^{2^s} acts on W as c and $\underline{c}\phi = \underline{c}$ so c must be equal to $a_{2^s} z^{\eta}$ for some $\eta \in \{0,1\}$ where $Z(T) = \langle z\rangle$. Then $c\phi = a_{2^s}\phi . z^{\eta} = a_{2^s} . a_{1+2^s} . z^{\eta} = a_{2^s} . z^{\eta} = c$, which contradicts the hypothesis of the theorem.

Thus we may assume that $W \neq A$. Then the remarks on the second page of this proof show that $\underline{W} \cap \underline{W}^{\perp} \neq 1$. I claim that there is some direct summand $\underline{X}_j$ of $\underline{A}$ such that $\underline{W} \cap \underline{X}_j^{\perp} = 1$. For otherwise, since for each j $\underline{W} \cap \underline{X}_j^{\perp}$ is a $K\langle\phi\rangle$ submodule of $\underline{W}$ we would have $1 \neq \underline{W}_{2^s} = \langle \underline{a}_{2^s}\rangle \leq \underline{X}_j^{\perp}$ for all $1 \leq j \leq t$ and hence $1 \neq \underline{W}_{2^s} \leq A^{\perp}$, which is impossible. So let $\underline{X}_j = \underline{U}$ generated by $\underline{b}_1$ say, and let $b_1, \ldots, b_t$ be defined by $b_{i+1} = b_i^{-1} . b_i\phi$ where $b_t = 1$. Let $\underline{b}_1, \ldots, \underline{b}_k$ form a K base for $\underline{U}$, and let $U_i = \langle b_i, \ldots, b_t\rangle$ for $1 \leq i \leq k+1$.

We continue by examining the relationship between U and W . $\underline{W} \cap \underline{U}^{\perp} = 1$ so $[\underline{W}_{2^s}, \underline{U}] \neq 1$. Applying (1) shows that $[\underline{W}_{2^s}, \underline{U}] = [\underline{W}, \underline{U}_{2^s}]$ so $[\underline{W}, \underline{U}_{2^s}] \neq 1$. Thus as $U_{k+1} \leq Z(T)$ we must have $k \geq 2^s$. However as $\underline{U}$ is an indecomposable $K\langle\phi\rangle$ module $k \leq 2^s$ and so $k = 2^s$.

As $[\underline{W}_{2^s},\underline{U}] \neq 1$, $[\underline{a}_{2^s},\underline{U}] \neq 1$. I claim that this happens whenever $[\underline{a}_{2^s},\underline{b}_1] \neq 1$. To show this we show that if $[\underline{a}_{2^s},\underline{b}_1] = 1$ then $[\underline{a}_{2^s},\underline{b}_i] = 1$ for all $i \geq 1$, so $[\underline{a}_{2^s},\underline{U}] = 1$. For if $1 = [a_{2^s},b_i]$ for some $1 \leq i \leq k$ then $1 = [a_{2^s},b_i] = [a_{2^s},b_i b_{i+1}]$ $= [a_{2^s},b_{i+1}]$, so if $1 = [\underline{a}_{2^s},\underline{b}_1]$ then $[\underline{a}_{2^s},\underline{U}] = 1$. Thus we may assume that $[\underline{a}_{2^s},\underline{b}_1] \neq 1$, and similarly that $[\underline{a}_1,\underline{b}_{2^s}] \neq 1$. (4)

Similar calculations show that $(\underline{U}.\underline{W}) \cap (\underline{U}.\underline{W})^{\perp} = 1$, for if not then $(\underline{U}.\underline{W})$ must contain a non-trivial element of $(\underline{U}.\underline{W})^{\perp}$ which is fixed under the action of ϕ , so must contain a non-trivial element of $\underline{B} = \underline{U}_{2^s}.\underline{W}_{2^s} = \langle \underline{a}_{2^s},\underline{b}_{2^s} \rangle$. But $\underline{a}_{2^s} \in \underline{W}^{\perp}$ so $[\underline{a}_{2^s}\underline{b}_{2^s},\underline{W}] = [\underline{b}_{2^s},\underline{W}] = [U,\underline{a}_{2^s}] \neq 1$ and no non-trivial element of $\underline{B}$ can lie in $(\underline{U}.\underline{W})^{\perp}$ and $(\underline{U}.\underline{W}) \cap (\underline{U}.\underline{W})^{\perp} = 1$. It follows from our remarks on the second page of the proof that $\underline{U}.\underline{W} = A$. We calculate the action of ϕ^{2^s} on $\underline{U}$ and $\underline{W}$, by using (3) . $\underline{U} \cap \underline{U}^{\perp}$ and $\underline{W} \cap \underline{W}^{\perp}$ are non-trivial so (ii) shows that $a^2_{1+2^{s-1}} = b^2_{1+2^{s-1}} = 1$, and so $a_1\phi^{2^s} = a_1.a_{1+2^s}$, $b_1\phi^{2^s} = b_1.b_{1+2^s}$ and

$a_i\phi^{2^s} = a_i$, $b_j\phi^{2^s} = b_j$ for $i,j \geq 2$, by (3).

Now ϕ^{2^s} acts non-trivially on W so $a_{1+2^s} = z$; let $b_{1+2^s} = z^{\eta}$ for some $\eta \in \{0,1\}$.

Now ϕ^{2^s} acts on T as conjugation by c and c centralises $U_2.W_2$ so it is easy to check that $\underline{c} \in \underline{B}$. It follows that we may assume that $c = a_{2^s}^{\eta}.b_{2^s}$. For

$a_1^{\,c} = a_1^{(b_{2^s})}$ as $a_{2^s} \in W^{\perp}$

$= a_1 z$ as $[a_1,b_{2^s}] \neq 1$.(4) and

$b_1^{\,c} = b_1^{(a_{2^s})^{\eta}}$ as $b_{2^s} \in U^{\perp}$

$= b_1 z^{\eta}$ as $[a_{2^s},b_1] \neq 1$ (4) .

But then $c\phi = (a_{2s}.a_{1+2s})^{\eta}.b_{2s}.b_{1+2s}$

$= a_{2s}.b_{2s}.z^{\eta}.z^{\eta}$

$= c$ (as $z^{2\eta} = 1$) which contradicts the hypothesis of the theorem.

We have now proved

5.2.5 Theorem Let G be an infinite non-cyclic finitely generated nilpotent group whose torsion subgroup has nilpotency class at most two . Then G admits a non-inner automorphism which acts nilpotently.

Proof If G has Hirsch length at least 2 then the result was given in chapter 1 . If G has Hirsch length one and is non-cyclic then the torsion subgroup is non-trivial; if the torsion subgroup is abelian the result was proved in 3.2.2 . If the torsion subgroup is nilpotent of class two then the result is proved if we can show that there does not exist an admissible pair (T,ϕ) with T a p-group of nilpotency class two. (3.3.2) . 5.2.3 shows that if such an admissible pair exists then T is an extraspecial 2-group. However if (T,ϕ) is admissible and T is extraspecial then T and ϕ must satisfy the conditions of 5.2.4 , which is impossible, so such an admissible pair cannot exist and G admits a non-inner automorphism.

More generally we have proved

5.2.6 **Theorem** Let G be a finitely generated nilpotent group of order at least three whose torsion subgroup has nilpotency class at most two. Then G admits a non-inner automorphism.

Proof If G is infinite and non-cyclic the result follows from the previous theorem and if G is infinite and cyclic the result is obvious. If G is finite the result follows from 2.3.5 .

Section 5.3

In this short section we examine another class of p-groups which can be treated with the methods developed so far. Let $\mathcal{J}$ be the class of finite p-groups T satisfying $\operatorname{rank} Z(T) \geqslant \operatorname{rank} Z_2(T)/Z(T)$. $\mathcal{J}$ includes all p-groups of maximal class and order at least p^4 , where a p-group of order p^n is said to be of maximal class if it has class $n-1$. For it can be shown that in a p-group of maximal class the lower and upper central series coincide and the non-trivial factors of the lower central series are cyclic of order p except for the first, which is elementary abelian of order p^2 .

We shall show that if (T,ϕ) is admissible then T is not an element of $\mathcal{J}$, and hence deduce that if (T,ϕ) is admissible then T does not have maximal class.

5.3.1 <u>Theorem</u> Let (T,ϕ) be an admissible pair . Then T does not lie in $\mathcal{J}$.

<u>Proof</u> Suppose that (T,ϕ) is an admissible pair and that $T \in \mathcal{J}$. We consider first the case when $Z(T)$ is not cyclic, and apply 4.2.5 . T is admissible so non-cyclic and $d = \operatorname{rank}(T/\Phi(T)) \geqslant 2$. Let $e = \operatorname{rank} Z(T)$; then as $T \in \mathcal{J}$ $\operatorname{rank}(Z_2(T)/Z(T)) \leqslant e$ and so $\operatorname{rank}(Z_2(T)/Z(T)) < de$. If $Z(T)$ is not cyclic then $e \geqslant 2$ and applying B2 of 4.2.5 we see that
$\operatorname{rank} Z_2(T)/Z(T) \geqslant de+3-e'-d'$ where e', d' are the ϕ-heights of $\Omega_1(Z(T))$ and $T/\Phi(T)$ respectively. As $e \geqslant e'$ and $d \geqslant d'$ we have $e \geqslant de+3-e-d$, that is $-1 \geqslant (d-2)(e-1)$. But $d \geqslant 2$ and $e \geqslant 2$ so this is impossible, and $Z(T)$ must be cyclic.

As $T \in \mathcal{J}$ and $Z(T)$ is cyclic $Z_2(T)/Z(T)$ must be cyclic. Let $Y/Z(T) = \Omega_1(Z_2(T)/Z(T)) \cong C_p$. Then $\mho_1(Y) \leq Z(T)$. As T is not exceptional 5.1.1 allows us to assume that Y contains a subgroup isomorphic to $C_p \times C_p$ so $p^2 \leq |\Omega_1(Y)| = |Y/\mho_1(Y)|$ and $\mho_1(Y)$ is a proper subgroup of $Z(T)$.

T is not of nilpotency class two as otherwise we would have $T/Z(T) = Z_2(T)/Z(T)$ and $T/Z(T)$ would be a non-trivial cyclic group which is impossible. Thus $T' \nleq Z(T)$ so $Y/Z(T) \leq T'.Z(T)/Z(T)$ and since $Z(T) \leq \Phi(T)$ by 4.2.4 we have $Y \leq T'.Z(T) \leq \Phi(T)$.

We now consider the subgroup
$H = \{\alpha \in \mathrm{Aut}T \; t^{-1}.t\alpha \in \Omega_1(Z(T)) \; \forall \; t \in T\}$ of AutT which was examined in section 4.2. $\mathrm{rank}Z_2(T)/Z(T) < de$ so $H \nleq \mathrm{Inn}T$, in fact $H \cap \mathrm{Inn}T \cong Y/Z(T)$. Then 3.3.9 shows that there exists $\beta \in H$ such that if $[\phi, \beta] = \mu_y \in H \cap \mathrm{Inn}T$ then $Z(T)$ is generated as a $\mathbb{Z}\langle\phi\rangle$ module by $v.v\beta. \ldots .v\beta^{p-1}$ where $v \equiv y$ modulo $Z(T)$. Now $v \equiv y$ modulo $Z(T)$ so $v \in Y \leq \Phi(T)$ and $v\beta = v$. Thus $Z(T)$ is generated as a $\mathbb{Z}\langle\phi\rangle$ module by v^p and so $Z(T) \leq \mho_1(Y)$.
But we have shown above that this cannot happen, so we conclude that $T \notin \mathcal{J}$.

We have now proved the following result.

5.3.2 Theorem Let G be a finitely generated nilpotent group whose torsion subgroup T is a p-group satisfying either a) $T \in \mathcal{J}$ or b) T has maximal class. Then G admits a non-inner automorphism which acts nilpotently.

Proof It suffices to show that if (T,ϕ) is an admissible pair then T cannot satisfy a) or b). If $T \in \mathcal{J}$ then the previous result shows that (T,ϕ) is not admissible. If T has maximal class then $T \in \mathcal{T}$ unless $T \leqslant p^3$ when T has class at most 2 and the result follows from 5.2.6 .

Section 5.4

Let us consider what we now know about automorphisms of finitely generated nilpotent groups of Hirsch length one. We have proved that certain classes of these groups admit non-inner automorphisms; the following theorem summarises our results.

5.4.1 <u>Theorem</u> Let G be a non-cyclic finitely generated nilpotent group of Hirsch length one and suppose that T the torsion subgroup of G satisfies one of the following conditions. Then G admits a non-inner automorphism acting nilpotently.

i) T is abelian

ii) T has nilpotency class 2

iii) T has exponent p

iv) $\Omega_1(Z(T)) \not\leq T'$

v) $Z(T) \not\leq \Phi(T)$

vi) T is metacyclic and $p \neq 2$

vii) T' is cyclic and $p \neq 2$

viii) T has maximal class

ix) $\mathrm{rank}(Z_2(T)/Z(T)) \leqslant \mathrm{rank}(Z(T))$.

<u>Proof</u> i follows from 3.2.2, ii from 5.2.5, iii and iv from 4.1.4, v from 4.2.4, vi and vii from 5.1.3 and vii and ix from 5.3.2 .

We have shown that to find a counterexample to the conjecture that any non-cyclic infinite finitely generated nilpotent group admits a non-inner automorphism acting nilpotently we need to find a finite p-group T and an automorphism ϕ of T of p-power order such that the pair (T,ϕ) is admissible, and we have established some properties of an admissible pair.

5.4.2 <u>Theorem</u> Let (T,ϕ) be admissible and let T be a p-group with d generators whose centre has rank e. Let the ϕ-heights of the $K\langle\phi\rangle$ modules $T/\Phi(T)$ and $\Omega_1(Z(T))$ be d' and e' respectively, where K is the field of p-elements. Then T has the following properties

i) any Sylow p-subgroup of OutT has cyclic centre

ii) T has nilpotency class at least three

iii) $\Omega_1(Z(T)) \leq T'$ and $Z(T) \leq \Phi(T)$

iv) if T is not a 2-group either $\operatorname{rank}(Z_2(T)/Z(T)) = de$ or $de > \operatorname{rank}(Z_2(T)/Z(T)) \geqslant de - d' - e' + 3$

vv) if T is not a 2-group then T' is not cyclic .

<u>Proof</u> i) If some Sylow p-subgroup of OutT does not have cyclic centre then the Sylow p-subgroup of OutT containing $\langle\bar{\phi}\rangle$ does not have cyclic centre and a Sylow p-subgroup of $C_{\mathrm{OutT}}(\bar{\phi})$ cannot be cyclic, contradicting the definition of admissible pair.
ii , iii and v follow from i ,ii ,iv ,v and vii of the previous theorem and iv follows from 4.2.5 .

The techniques we have used in this essay depended, more or less, on finding suitable elementary abelian p-subgroups of the automorphism group of T which do not lie in InnT, and using these to calculate the action of ϕ . It seems plausible that with a little more work these methods could be extended to show that if (T,ϕ) is admissible then T cannot be a regular p-group (in the sense of Hall) To develop the method further it might also be worth investigating the elements of AutT of order p which do not lie in InnT . Whether such elements always exist (when T does not have order p) does not seem to be known.

However it seems unlikely that these ideas will be able to give a complete solution to the problem; in particular it is hard to believe that the general case can be solved without the introduction of some inductive arguments. Although it is difficult to formulate reasonable inductive hypotheses involving admissible pairs the argument of 5.2.4 , in which we showed that if (T,ϕ) is admissible then (T,ϕ) cannot be an extraspecial 2-group showed that under certain circumstances this can be done. It seems to me that to extend the results of this essay in any significant way one may need to vary the definition of an admissible pair in some way in order to work with p-groups satisfying some condition which is more amenable to inductive arguments.

In chapter 2 we discussed cohomological techniques for dealing with group automorphisms and it may be that these will be the methods which eventually solve the problem. We showed that if G is a finitely generated nilpotent group of Hirsch length one and if S is a certain finite quotient of G then any non-inner automorphism of S which acts on S/S' in a certain way lifts to a non-inner automorphism of G . An examination of the proof reveals that if T is the torsion subgroup of G and ϕ is the automorphism of T induced by conjugation by a generator of G/T then any $\rho \in \mathrm{Aut}T$ with $[\rho,\phi] \in \mathrm{Inn}T$ and $\langle\bar{\rho}\rangle \nleq \langle\bar{\phi}\rangle \leq \mathrm{Out}T$ will induce an automorphism of G acting on some finite quotient in the required way , and we may regard the two approaches as essentially the same. However the advantage of looking at the finite quotient S is that in particular any non-inner

References

1 G.Baumslag — Lecture notes on nilpotent groups , Regional conference series in mathematics (2) 1971

2 W.Gaschütz — Kohomologische Trivialitaten und aussere Automorphismen von p-gruppen, Math. Z. 88 1965 , 432-433.

3 W.Gaschütz — Nichtabelsche p-gruppen besitzen aussere p-automorphismen. J. Algebra 4 (1966), 1-2.

4 D.Gorenstein — Finite Groups, Harper and Row.

5 K.W.Gruenberg — Cohomological topics in group theory, Lecture notes in Mathematics 143, Springer, Berlin (1970)

6 H.Heineken — Automorphism groups of torsion-free nilpotent groups of class 2, Symposia Math. (1976), 235-250.

7 D.J.S.Robinson — A contribution to the theory of groups with finitely many automorphisms, Proc. London Math. Soc. (3) 34 (1977), 34-54.

8 E.Schenkman — The existence of outer automorphisms of some nilpotent groups of class two, Proc. Amer. Math. Soc. 6 (1955), 6-11 .

9 P.Schmid — Normal p-subgroups in the group of outer automorphisms of a finite p-group, Math.Z.

10 S.E.Stonehewer and N.D.Gupta — Outer automorphisms of some finitely generated nilpotent groups, Arch. Math. (to appear)

11 C.Wells — Automorphisms of group extensions, Trans. Amer. Math. Soc. 155 (1971) 189-194

12 H.Wielandt — Eine Varallgemeinerung der invarianten Untergruppen, Math. Z. 45 (1939), 209-244 .

13 A.E.Zalesskii — A nilpotent p-group possesses an outer automorphism, Dokl. Akad. Nauk SSSR 196 (1971) 751-754 = Soviet Math Dokl. 12 (1971) 227-230.

14 A.E.Zalesskii — An example of a torsion-free nilpotent group having no outer automorphisms. Mat. Zametki 11 (1972), 21-26 = Math.Notes 11 (1972), 16-19.

Summary of notation

If G is group and B is a subset of G then $\langle B \rangle$ denotes the subgroup of G generated by B . If a and b are elements of G then $a^b = b^{-1}ab$ and $[a,b] = a^{-1}a^b$ and if A and B are subsets of G then $[A,B]$ denotes $\langle [a,b] \mid a \in A, b \in B \rangle$. $[G,G]$ is denoted by G'. The elements of the upper central series of G are denoted by $Z_i(G)$ for $i \geqslant 1$ where $Z(G) = Z_1(G) = \langle a \in G \mid [a,G] = 1 \rangle$ and $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$.

If G is a p-group then $\Omega_i(G) = \langle g \in G \mid g^{p^i} = 1 \rangle$ and $\mho_i(G) = \langle g \in G \mid g = h^{p^i}$ for some $h \in G \rangle$. Then the Frattini subgroup of G is denoted by $\Phi(G) = G'.\mho_1(G)$. If X is an abelian section of G and $\Omega_1(X)$ has order p^x then x is called the rank of X . The exponent of G is the smallest integer n such that $g^n = 1$ for all $g \in G$.

AutG denotes the group of automorphisms of a group G and InnG the group of inner automorphisms of G ; if $g \in G$ then conjugation by g is denoted by $\mu_g \in$ InnG . NilG denotes the subset of AutG consisting of automorphisms of G which act nilp nilpotently on G . If H is a subset of G then $N_{AutG}(H) = \{\alpha \in AutG \mid H\alpha = H\}$ and $C_{AutG}(H) = \{\alpha \in AutG \mid h\alpha = h \ \forall h \in H\}$. If $InnG \leq N_{AutG}(H)$ then $N_{OutG}(H)$ denotes $N_{AutG}(H)/InnG$. If $\beta \in AutG$ and H is a subset of G then $[\beta,H] = \langle b^{-1}\beta.b \mid b \in H \rangle$. OutG denotes AutG/InnG .